**Centro Universitário de Brasília**
**Instituto CEUB de Pesquisa e Desenvolvimento - ICPD**

**AUGUSTO CÉSAR GONÇALVES DE AZEVEDO**

# ADOÇÃO DE PROTOCOLOS DE SEGURANÇA EM REDES IEEE 802.11 NO PLANO PILOTO EM BRASÍLIA

Brasília
2014

**AUGUSTO CÉSAR GONÇALVES DE AZEVEDO**

# ADOÇÃO DE PROTOCOLOS DE SEGURANÇA EM REDES IEEE 802.11 NO PLANO PILOTO EM BRASÍLIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Marco Antônio de O. Araújo

Brasília
2014

**AUGUSTO CÉSAR GONÇALVES DE AZEVEDO**

# ADOÇÃO DE PROTOCOLOS DE SEGURANÇA EM REDES IEEE 802.11 NO PLANO PILOTO EM BRASÍLIA

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança.

Orientador: Prof. MSc. Marco Antônio de O. Araújo

Brasília, 27 de Março de 2014.

**Banca Examinadora**

_____

Prof. MSc. Francisco Javier de Obaldia Díaz

_____

Prof. Dr. Gilson Ciarallo

## RESUMO

Segurança em redes sem fio é um assunto cada vez mais em evidência. A popularização das redes Wi-Fi é um fenômeno impulsionado pela necessidade de mobilidade trazida por um número cada vez maior de dispositivos como celulares e *tablets*. A ampla difusão desta tecnologia é evidenciada pelos dados apresentados neste estudo. Sua presença ocorre de forma cada vez mais ubíqua, e seu uso é cada vez mais natural. Passa-se a interagir com a tecnologia de forma mais mecânica e automática. Muitas vezes não se faz a devida análise quanto aos riscos inerentes a sua utilização. Este estudo provê um entendimento melhor destes riscos, por vezes associados à perda de confidencialidade e acesso não autorizado a ambientes lógicos. Identifica também a atuação dos protocolos de segurança presentes na especificação IEEE 802.11 na mitigação destes riscos. Analisa seus pontos de sucesso e falha. Adota uma abordagem prática para verificar sua presença na região do Plano Piloto em Brasília, Distrito Federal, Brasil. Compara três diferentes cenários de uso, delimitados com base na destinação dos setores da cidade conforme planejamento urbanístico: o primeiro composto por usuários predominantemente residenciais, o segundo por médias e grandes empresas e um terceiro por entidades ligadas ao governo. Com base nas informações coletadas de 12.859 pontos de acesso, observou-se que apenas 3,35% das redes localizadas em áreas residenciais encontravam-se sem nenhum tipo de proteção. Viu-se também que o uso do protocolo WEP ainda é expressivo, encontrado em 5% do total das redes analisadas. Observou-se também que a adoção do WPA2 ultrapassa 68% do total das redes. Constatou-se o uso de senha compartilhada para proteção da rede em 70% dos casos observados. Identificou-se a região central da cidade como sendo a área de maior densidade de redes dentre as áreas observadas. Observou-se também que as empresas de telecomunicação estão contribuindo para o aumento da segurança das redes sem fio ao fornecerem, como parte de seus serviços, equipamentos e instalação. As análises realizadas possibilitaram uma compreensão melhor da aplicação dos protocolos nas redes da cidade.



**Palavras-chave**: Wi-Fi, segurança, *wardrive*, riscos, Brasília.

## ABSTRACT

Security in wireless networks is a increasingly evident subject. The widespread adoption of Wi-Fi is a phenomenon driven by the need for mobility brought by an increasing number of devices such as mobile phones and tablets. This phenomenon is evidenced by the data presented in this study. Wi-Fi networks are more ubiquitous, and its use is becoming more natural. Our interaction with technology occurs in a more mechanical and automatic way. Because of that we often do not analyze the risks inherent its use. This study gives a better understanding of these risks. Often associated with loss of confidentiality and unauthorized access to logical environments. Also identifies how security protocols present in the IEEE 802.11 specification contributes to mitigate these risks. Analyzes where they are successful and where they fail. Adopts a practical approach to verify their presence in the city of Brasilia, Distrito Federal, Brazil. It compares three different scenarios of use, delimited on the basis of allocation of the sectors in the city's urban plan: the first consists of predominantly residential users; the second, of medium and large companies and the third, of entities linked to the government. Based on information collected from 12,859 access points, only 3.35% of the networks located in residential areas were found without any protection. We saw also that the use of WEP is yet expressive. It were found in 5% of the analyzed networks. The adoption of WPA2 exceeds 68% of total networks. The use of Pre-Shared Keys occurs in 70% of cases observed. We found the central region of the city as the area of highest density of networks among the observed. Also noted that telecommunications companies are contributing to the increased security of wireless networks providing equipment and deploiment as services. The analysis performed allowed a better understanding of the implementation of the protocols in the networks of the city .



**Key words**: Wi-Fi, security, wardrive, risks, Brasília

**SUMÁRIO**

# INTRODUÇÃO

Cresce a cada dia o volume de informações armazenadas em mídias digitais. A cultura de uso das redes sociais estimula a produção e o compartilhamento de informações à medida em que introduz novos hábitos como o compartilhamento instantâneo de fotos e vídeos. Esse fenômeno é alavancado pela evolução das tecnologias de telecomunicação e de dispositivos móveis de uso pessoal como smartphones e *tablets*. Com o aumento do número destes dispositivos cresce também a demanda do uso de redes sem fio, que trazem comodidade pela facilidade de instalação e configuração, bem como mobilidade, permitindo ao usuário que se locomova dentro da área de cobertura da rede sem perder o acesso aos serviços que ela provê (RUFINO, 2011).

Conforme Tanenbaum e Wetherall (2011), a principal aplicação das redes sem fio é viabilizar a conexão de dispositivos a internet, o que faz das redes sociais e das redes sem fio duas tecnologias convergentes.

Esse contexto traz novas questões relacionadas à privacidade dos usuários e à segurança das informações trafegadas. Como o meio de transmissão é o ar, a grande questão é como impedir que usuários desconhecidos tenham acesso aos dados da rede (RUFINO, 2011).

O utilização de redes Wi-Fi é cada vez mais comum em ambientes corporativos, comerciais e residenciais, porém a grande maioria dos usuários não está ciente dos riscos a que estão expostos ao fazerem uso desta tecnologia.

As redes sem fio transpõem barreiras físicas ampliando as capacidades de comunicação e ao mesmo tempo dificultando o controle sobre quem tem acesso às informações trafegadas neste canal de comunicação. É difícil controlar o que não se vê. Daí a importância dos protocolos de segurança que fazem uso de criptografia para prover autenticação dos usuários conectados a essas redes, bem como o sigilo dos dados trafegados. Muitos desses protocolos de segurança hoje utilizados das redes sem fio foram comprometidos.

É sabido que existem falhas graves em alguns dos protocolos de segurança implementados em grande parte dos equipamentos usados para

provimento de pontos de acesso a redes sem fio. Essas falhas criam possibilidades para o roubo de dados, acessos não autorizados à rede, dentre muitas outras. Boa parte dos problemas de segurança podem ser drasticamente minimizados por meio da realização de ajustes na configuração desses dispositivos. Não espera-se que usuários domésticos tenham conhecimento de como realizar tais procedimentos, entretanto pode-se adotar medidas, tais como, a melhoria das configurações de fábrica que acompanham os equipamentos. Já das empresas espera-se maior competência técnica na realização da implantação de uma rede sem fio, seja ela para fins de utilização pública ou interna à própria organização.

A proposta do presente estudo é compreender melhor os riscos e ameaças a que estão sujeitos os usuários de redes Wi-Fi. Para isso é necessário conhecer seu funcionamento e principalmente os mecanismos de proteção existentes. O foco maior será nos protocolos de segurança do 802.11, suas vulnerabilidade e alguns ataques a que estão sujeitos.

Os objetivos do presente trabalho são: observar as configurações de segurança de pontos de acesso a redes sem fio 802.11 na região do Plano Piloto em Brasília no Distrito Federal; identificar os protocolos de segurança mais utilizados; identificar áreas de maior densidade de redes sem fio e comparar as configurações encontradas em áreas residenciais, áreas destinadas a empresas e também órgãos governamentais.

Para se verificar a qualidade dos aspectos de segurança das redes Wi-Fi do Plano Piloto em Brasília foi utilizada a técnica conhecida como *Wardrive*. Essa técnica consiste na instalação, em um veículo, de equipamentos próprios para a identificação de redes sem fio. Com o veículo preparado, percorre-se o perímetro da área-alvo da análise para realização da captura de dados.

Para determinar a melhor configuração de equipamentos foi realizado um comparativo entre *softwares* que permitissem a coleta de dados, bem como *hardware* necessário (placas de rede, antenas e sistema de GPS), conforme detalhamento no capítulo 4. Uma vez determinada a configuração a ser utilizada para realização da varredura, percorreu-se de carro um trajeto que cobrisse áreas da cidade destinadas a residências, grandes e médias empresas e órgãos governamentais.

Espera-se demonstrar com este estudo a importância da adoção de padrões fortes de segurança no uso de redes sem fio, chamar a atenção das pessoas para os riscos relativos a quebra de privacidade e possibilidade de que terceiros consigam acesso não autorizado às suas redes privadas, seja para realização de ilícitos, seja para qualquer outra finalidade.

O presente trabalho foi então estruturado em 4 capítulos.

No primeiro capítulo, apresentam-se características gerais do funcionamento das redes sem fio do padrão IEEE 802.11, introduzindo as principais versões e protocolos de segurança; no segundo capítulo faz-se uma análise sobre riscos e ameaças, apresentando uma taxonomia para ataques a redes sem fio e alguns dos principais ataques e vulnerabilidades a que estão sujeitas; no terceiro capítulo, são apresentados alguns conceitos de segurança da informação e em seguida é detalhado o funcionamento dos protocolos de segurança do 802.11, evidenciando vulnerabilidades conhecidas; no quarto e último capítulo apresenta-se como estudo de caso a avaliação dos protocolos de segurança adotados em redes do Plano Piloto em Brasília; neste mesmo capítulo são apresentados os resultados da análise realizada em cima dos dados coletados utilizando-se a técnica de *Wardrive*.

# 1 REDES SEM FIO IEEE 802.11

Mais conhecido como Wi-fi, 802.11 é o conjunto de padrões mais difundido até o momento para implementação de redes locais sem fio, também conhecidas como WLANs (*Wireless Local Area Networks*). O desenvolvimento destes padrões é realizado por um grupo de trabalho vinculado ao Instituto de Engenharia Elétrica e Eletrônica (IEEE). Esse grupo também é responsável pelo desenvolvimento de guias, recomendações e melhores práticas para implementação dos padrões desenvolvidos.

O 802.11 foi projetado para interoperar com as redes cabeadas tradicionais e atua principalmente na camada física com as especificações PHY (de *physical layer*) e de enlace, com a especificação da subcamada MAC (*media access control*). As especificações abordam diversos aspectos como multiplexação, segurança do canal de comunicação, interoperabilidade entre dispositivos e até mesmo QoS (*Quality of Service*), cujo objetivo é definir mecanismos para priorização dos recursos da rede.

## 1.1 Principais características

Segundo Kurose e Ross (2006) o elemento fundamental da arquitetura do 802.11 é o “conjunto básico de serviço” (*basic service set* - BSS) que contém uma ou mais estações sem fio e uma estação base central, conhecida como ponto de acesso (*acces point* - AP).

A respeito do funcionamento das redes 802.11, Kurose e Ross (2006, p. 402) descrevem:

> Como acontece em dispositivos Ethernet, cada estação sem fio 802.11 tem um endereço MAC de 6 bytes que é armazenado no suporte lógico inalterável (firmware) do adaptador da estação. [...] Cada AP também tem um endereço MAC para sua interface sem fio. Como na Ethernet, esses endereços são administrados pelo IEEE e são (em teoria) globalmente exclusivos.

Rufino (2011) aponta que os endereços MAC dos dispositivos são transmitidos em claro durante as comunicações sem fio, o que gera vulnerabilidades

pois permite que equipamentos não associados a rede possam identificar os endereços MAC de dispositivos que estão associados e eventualmente assumirem a identidade de um destes equipamentos.

Os padrões desenvolvidos até o momento dentro da família 802.11 operam nas frequências 2,4GHz e 5GHz que, segundo convenções internacionais podem ser utilizadas sem a necessidade de obter licença de uma agência governamental, no caso do Brasil a ANATEL (RUFINO, 2011). Com o objetivo de aumentar a eficiência nas comunicações e diminuir a interferência entre dispositivos, estas faixas de frequências são subdivididas em faixas menores chamadas de canais, geralmente com 20MHz ou 40MHz nas versões mais recentes.

Por operar em frequências abertas, as redes 802.11 concorrem com outros dispositivos e serviços que utilizam as mesmas faixas de frequência como telefones sem fio e dispositivos com tecnologia Bluetooth. Segundo Rufino (2011) a faixa de frequência de 2,4GHz é utilizada por uma vasta quantidade de equipamentos e por isso, diz-se que é poluída ou suja. Inclusive APs pertencentes a redes diferentes podem causar interferência um no outro.

Kurose e Ross (2006) definem como selva de Wi-Fis (Wi-Fi *jungle*) o cenário em que para uma dada localização física uma estação recebe sinal suficientemente forte de dois ou mais APs, cenário em que é possível que um AP interfira na comunicação do outro. Encontrar situações típicas de uma selva de Wi-Fis é comum em muitas áreas comerciais e residenciais do Distrito Federal e do Brasil em geral, deixando de ser características apenas de grandes cidades de países ricos como Nova Iorque, utilizada como exemplo pelo autor.

Com relação ao isolamento dos sinais nas redes sem fio Rufino (2011, p. 19) afirma que:

> Nas redes convencionais, os cabos podem se valer de diversos tipos de materiais para proteção física, isolando, tanto quanto for a qualidade do material, o que ali trafega do resto do ambiente. Já com redes sem fio, a informação não dispõe de nenhuma proteção física, mas, por outro lado, pode atingir, sem muito esforço, locais de difícil acesso para redes cabeadas.

As redes sem fio no padrão 802.11 possuem raio de alcance de até 100 metros em ambientes fechados, podendo atingir distancias significativamente

maiores em espaços abertos e com antenas específicas. Com relação à propagação do sinal de radiofrequência Rufino (2011, p. 20) afirma que:

> Quando falamos de frequências de rádio temos em mente que um sinal será propagado no espaço por alguns centímetros ou por vários quilômetros. A distância percorrida está diretamente ligada a frequência do sinal. Em tese, quanto mais alta a frequência, menor será a distância alcançada.

Conforme exposto por Rufino (2011), a fórmula geral que define a proporção entre frequência do sinal e distância em um espaço livre, conforme o modelo Cost 231 – Walfish-Ikegami é:

PS = 32,4 + (20 log D) + (20 log F)

Onde:

PS = perda do sinal

D = distância em quilômetros

F = frequência em MHz

Além dos problemas de interferência, em redes Wi-fi o meio é compartilhado entre todas as estações conectadas a um mesmo concentrador. De modo que a quantidade de banda disponível para cada usuário diminui a medida que a quantidade de usuários aumenta (RUFINO, 2011).

O compartilhado do meio implica que todas os dispositivos no raio de acesso da rede estão recebendo todas as mensagens trafegadas. Devido a essa característica, uma estação pode capturar trafego não originado em si ou que não lhe seja destinado, de forma semelhante ao que acontece em um mesmo segmento de uma rede cabeada, o que representa um risco para a confidencialidade das comunicações (RUFINO, 2011).

Em se tratando de redes sem fio, esse problema assume uma dimensão ainda maior pois é muito difícil conter um sinal de rádio em um determinado perímetro, de modo que ele pode “vazar“ para fora do ambiente físico a que se destina. No caso de uma empresa ou entidade governamental as consequências podem ser ainda mais graves, pois, em geral, são trafegadas com um grau maior de sensibilidade. Atacar a rede também se torna mais fácil na medida em que não há mais necessidade de contato físico direto com os equipamentos (RUFINO, 2011).

O padrão em desenvolvimento 802.11ac, busca endereçar a questão do compartilhamento do meio propondo um método de direcionar o sinal apenas para os equipamentos que estão comunicando. Entretanto, o objetivo principal é melhorar o aproveitamento do meio para possibilitar velocidades maiores na comunicação. Como consequência, pode ser que ocorra alguma melhoria na segurança no caso em que se torne mais difícil capturar um sinal mais direcionado.

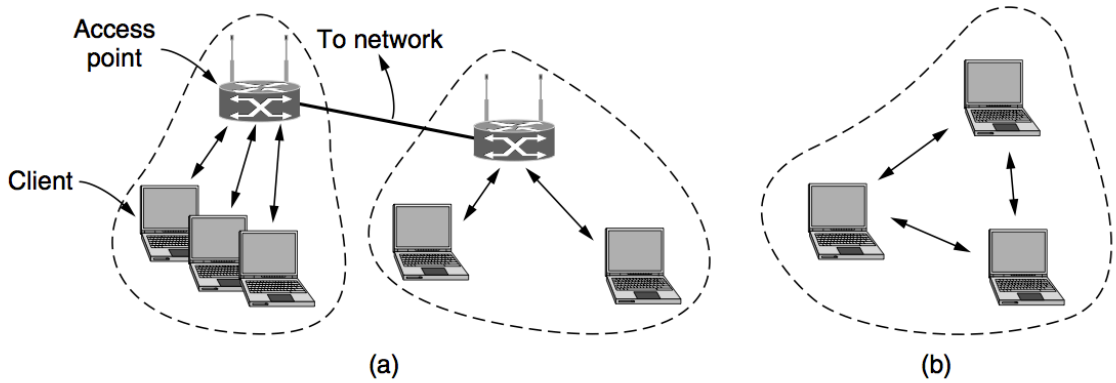
Os cenários apresentados até o momento já representam motivos suficientemente fortes para justificar a importância do investimento em mecanismos que realizem controle de acesso a estas redes, em conjunto com a utilização de padrões fortes de autenticação e mecanismos eficazes que permitam a garantia da confidencialidade dos dados trafegados.

## 1.2 Modo infraestrutura e modo Ad-Hoc

Conforme Tanenbaum e Wetherall (2011) as redes 802.11 podem ser utilizadas em dois modos. O primeiro e mais comum é o modo de infraestrutura, utilizado para conectar dispositivos como computadores e *smartphones* a outras redes por meio da associação de cada cliente a um AP. A topologia do modo infraestrutura está representada na figura 1 (a). Neste modo o cliente transmite e recebe seus pacotes por meio do AP. É possível ainda, conectar os AP's uns aos outros por meio de uma rede cabeada chamada rede de distribuição, criando o que o autor denomina rede 802.11 estendida. Este modo de operação em que existe um elemento que centraliza e controla a comunicação (AP) apresenta vantagens, pois permite que todas as configurações de segurança (como autenticação, autorização, controle de banda e criptografia) fiquem concentradas em um só ponto (RUFINO, 2011).

O segundo modo de funcionamento das redes sem fio é chamado "ad-hoc". Seu objetivo é formar uma rede de equipamentos conectados diretamente uns aos outros, sem a necessidade de uma infraestrutura central para realização da conexão, portanto não existem APs neste modo de operação. Tanenbaum e Wetherall (2011) afirmam também que este tipo de rede não é comum pois a principal aplicação das redes sem fio é viabilizar a conexão de dispositivos a internet.

Figura 1 – Arquitetura 802.11. (a) Modo de infraestrutura. (b) Modo Ad-Hoc.




Fonte – Retirado de Tanenbaum e Wetherall (2011, p. 188).

A ausência do concentrador de rede (AP), cria vários problemas de segurança, administração e gerência da rede (RUFINO, 2011). Dentre alguns deles pode-se citar problemas na identificação de elementos confiáveis na rede e dependência de elementos pares para realização do roteamento e tráfego de qualquer pacote. A dificuldade no controle da rede é ainda maior em cenários nos seus componentes são móveis, o que significa que podem entrar e sair do alcance dos demais elementos (e consequentemente da rede) a qualquer momento.

## 1.3 Versões do IEEE 802.11

O padrão IEEE 802.11 é a base para o desenvolvimento de produtos que utilizam redes sem fio com a marca Wi-Fi. Sua primeira versão foi publicada em 1997 e a partir dela, diversas emendas e revisões. Cada emenda é representada por caracteres do alfabeto, sem distinção de maiúsculas e minúsculas (entretanto geralmente são utilizados em minúsculo), atribuídas em ordem crescente. A todo momento existem diversas melhorias em proposição, que podem ser desenvolvias simultaneamente. Da mesma maneira, cada emenda pode tratar de pontos completamente distintos do funcionamento das redes se fio. Cada uma delas possui um grupo de trabalho associado e um sequencial de identificação, que é atribuído mesmo antes da versão ser aprovada e tornar-se, de fato, parte do padrão. Assim, é possível que ocorra o caso em que uma emenda com sequencial menor seja aprovada e lançada posteriormente a uma emenda com sequencial maior, cujos trabalhos tenham sido iniciados posteriormente. O que significa que não existe

necessariamente uma relação de dependência entre versões que estejam em desenvolvimento simultâneo.

Eventualmente é feita uma revisão geral do padrão em que são incorporadas todas as emendas aprovadas e publicadas até o momento da revisão. A revisão geralmente é identificada pelo ano e novas versões incorporam a versão anterior, que é automaticamente revogada. Para fins comerciais, o mercado trata cada emenda como um padrão específico. Isso ocorre, pois facilita a descrição das capacidades de um produto, na medida em que se associam ao produto as funcionalidades introduzidas em uma determinada emenda. Por isso se vê produtos exibindo selos com referência aos "padrões" 802.11b/g/n (ou qualquer outro conjunto), o que na prática significa que o produto implementa o padrão 802.11 compatível com as especificações constantes nas emendas "b", "g" e "n". Para fins didáticos, a partir deste parágrafo as emendas serão chamadas de padrão.

A implantação e difusão das alterações introduzidas por um novo padrão depende do mercado. No caso do 802.11b, sua difusão foi muito mais rápida do que a do 802.11a, apesar de sua proposição ter sido formalizada alguns meses depois do 802.11a e ambos terem sido aprovados conjuntamente. Atribui-se a difusão mais rápida do 802.11b ao menor custo para fabricação de seus componentes.

Outro caso interessante também é o do 802.11ac que cujo principal benefício é aumentar significativamente as velocidades de transmissão de dados em comparação às versões anteriores. Até o presente momento, em que este trabalho está sendo desenvolvido, o padrão 802.11ac ainda não foi aprovado, entretanto alguns fabricantes de equipamentos, a exemplo da empresa Apple, já se adiantaram e lançaram produtos no mercado com as tecnologias propostas na versão em desenvolvimento. Esse movimento é interessante quando o trabalho de proposição da emenda encontra-se adiantado e maduro o suficiente para que não sejam mais necessárias alterações de *hardware* além das já propostas. Isso permite que ajustes posteriores sejam feitos apenas com atualizações de *software* por meio da atualização do *firmware*[1] dos equipamentos.

[1] *Firmware* é o conjunto de instruções de programa de um determinado hardware implementado em uma estrutura de memória do tipo ROM (*Read-Only Memory*) que após gravada permite apenas a realização de leitura, ou Flash ROM que pode ser atualizada em eventual necessidade (PATTERSON; HENNESSY, 2005). O maioria dos dispositivos não necessita de atualizações de *firmware* ao longo de sua vida útil.

Uma nova emenda pode tratar de questões pontuais para resolver um determinado problema, a exemplo do 802.11z cujo objetivo foi habilitar os equipamentos a operar com a faixa de frequência de 3650MHz a 3700MHz (somente nos Estados Unidos), ou até mesmo propor grandes alterações que abranjam diversos pontos do funcionamentos das redes sem fio, como é o caso do 802.11ac.

Nas seções seguintes serão apresentadas algumas características dos principais padrões de funcionamento das redes sem fio. Será dado foco no funcionamento em modo de infraestrutura e aspectos de segurança relacionados.

### 1.3.1 *Aspectos da comunicação*

Em se tratando do funcionamento das redes sem fio os principais padrões são o “a”, “b”, “g”, “n” e “ac” (ainda não aprovado). Os dois principais fatores de diferenciação destas redes em termos de desempenho são os métodos de modulação e a presença da tecnologia MIMO (*multiple-input and multiple-output*).

O quadro 1 compara as principais características destes padrões.

Quadro 1 - Comparativo entre 802.11 “a”, “b”, “g”, “n” e “ac”.

| Protocolo 802.11 | Lançamento | Freq. (GHz) | Largura da faixa (MHz) | Taxa de dados por fluxo (Mbps) | Fluxos MIMO possíveis | Modulação |
|---|---|---|---|---|---|---|
| — | Jun 1997 | 2.4 | 20 | 1, 2 | 1 | DSSS, FHSS |
| a | Set 1999 | 5 | 20 | 6, 9, 12, 18, 24, 36, 48, 54 | 1 | OFDM |
| | | 3.7 | | | | |
| b | Set 1999 | 2.4 | 20 | 1, 2, 5.5, 11 | 1 | DSSS |
| g | Jun 2003 | 2.4 | 20 | 6, 9, 12, 18, 24, 36, 48, 54 | 1 | OFDM, DSSS |
| n | Out 2009 | 2.4/5 | 20 | 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 | 4 | OFDM |
| | | | 40 | 15, 30, 45, 60, 90, 120, 135, 150 | | |
| ac (proposta) | Dez 2012 | 5 | 20 | até 87.6 | 8 | |
| | | | 40 | até 200 | | |
| | | | 80 | até 433.3 | | |
| | | | 160 | até 866.7 | | |

Fonte – Adaptado de Wikipedia, com base em.

Com base no Quadro 1 é possível realizar algumas observações interessantes:

1. O padrão de modulação OFDM (*ortogonal frequency-division multiplexing*) é o que permite taxas de transmissão mais elevadas do que o DSSS (*direct-sequence spread spectrum*) e o FHSS (*frequency-hopping spread spectrum*);
2. A partir da verão “n”, foi introduzida a tecnologia MIMO, que utiliza múltiplas faixas de frequência para realização de transmissões em paralelo, desse modo atingindo maiores velocidades de transmissão e recepção. Na tabela é possível observar o aumento da largura de faixa utilizada a partir do padrão “n“;

### 1.3.2 *Aspectos da segurança*

Desde sua primeira versão o 802.11 aborda questões relativas a segurança das redes sem fio. O protocolo WEP (*Wired Equivalent Privacy*) foi o primeiro a surgir para agregar segurança a estas redes. Com o auxílio de uma chave simétrica compartilhada entre as estações de trabalho é realizado o controle de acesso ao meio, bem como a proteção dos dados trafegados com o auxílio de algoritmos de cifração (RC4), tendo em vista que estes podem ser capturados de forma passiva por qualquer dispositivo capaz de receber o sinal (RUFINO, 2012).

Hoje as vulnerabilidades deste mecanismo encontram-se amplamente documentadas, inclusive com diversos *softwares* de código aberto que exploram essas vulnerabilidade disponíveis livremente para *download* na *internet*. Dessa maneira fica evidente que o WEP não é mais capaz de prover segurança para as redes sem fio conforme relatado por Peisong e Guangxue (2010), Zhao e Shoniregun (2007) e diversos outros autores.

Após a divulgação de diversas vulnerabilidades do WEP foi proposta pela Wi-Fi Alliance[2] a implementação parcial do padrão em desenvolvimento 802.11i dando origem ao WPA (Wi-Fi *Protected Access*). O padrão “i“ introduz o protocolo de rede *Robust Security Network* (RSN) que cria uma camada de abstração para a

[2] Wi-fi Alliance é uma associação global, sem fins lucrativos, composta por centenas de empresas dedicadas a conectividade. É a maior responsável pela adoção em larga escala dos padrões 802.11, também conhecido como Wi-Fi. Essa organização detém os direitos sobre diversas marcas e logotipos relacionados a tecnologia, a exemplo do prórpio “Wi-Fi”, "Wi-Fi ZONE”, ‘WPA2“ e muitas outras.

utilização de mecanismos de segurança, de modo que permite a substituição dos métodos de proteção por outros mais atuais e eficazes de forma mais transparente (RUFINO, 2011).

Uma adição importante trazida pelo WAP é o TKIP (*Temporal Key Integrity Protocol*), utilizado para geração e troca constante das chaves de criptografia utilizadas pelos equipamentos na comunicação. Rufino (2011, p. 38) explica que o TKIP pode ser configurado para substituir o vetor de iniciação[3] a cada pacote, por sessão ou por período".

O WPA2 (Wi-Fi *Protected Access* 2) é a implementação completa do 802.11i que prevê o uso do padrão de criptografia AES (*Advanced Encryption Standard*) – que cifra em blocos, enquanto o WEP e WPA utilizam a cifra de fluxo[4] RC4 - atualmente quebrada. Entretanto, ataques práticos que permitam a quebra de confidencialidade ainda são pouco viáveis devido ao grande volume de dados cifrados necessários (ALFARDAN et al., 2013).

Outra adição importante do 802.11i foi o protocolo CCPM (*Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) que consiste em uma adaptação do AES para operar em modo contador associado a um mecanismo de verificação de integridade e autenticidade, o CBC-MAC[5] (SIVAKUMAR; VELMURUGAN, 2007).

Um dos focos importantes do padrão "i" é a autenticação de usuários, até então não coberta de forma efetiva pelo WEP. Para essa tarefa são utilizados em conjunto os padrões 802.1x, que encapsula quatro dos métodos de autenticação descritos no *Extensible Authentication Protocol* (EAP[6]), conforme Rufino (2011). O 802.1x é um protocolo anterior ao surgimento das redes sem fio, entretanto atua de

[3] Vetor de iniciação (ou inicialização) é um bloco de dados aleatório utilizado como entrada do primeiro bloco em criptosistemas de blocos encadeados, como o CBC (*Cipher-block chaining*), para conferir maior aleatoriedade ao processo, de modo que toda vez que um mesmo dado for cifrado com uma determinada chave o resultado será diferente para diferentes vetores de inicialização.

[4] Umas das grandes diferenças entre cifras de bloco e de fluxo é a quantidade de bytes cifradas em cada iteração do algoritmo. Em geral o tamanho dos blocos é de pelo menos 64bits (128 no caso do AES), o que significa que a cada iteração o algoritmo cifrará a quantidade de bits correspondente ao tamanho do bloco (TANENBAUM; WETHERALL, 2011). Essa abordagem aumenta a entropia da cifra em comparação as cifras de fluxo que operam byte a byte.

[5] O CBC-MAC é um tipo de código de autenticação de mensagens que consiste do último bloco resultante da execução de uma cifra em modo de encadeamento blocos de cifras (CBC – *Cypher Block Chaining*) como demonstrado por Sivakumar e Velmurugan (2007).

[6] O Protocolo Extensível de Autenticação (*Extensible Authentication Protocol* - EAP) é descrito na RFC3748 e atualizado na RFC5247.

forma complementar, permitindo a realização de autenticação por meio de métodos já consolidados, a exemplo do RADIUS (*Remote Authentication Dial-in User Service*). O RADIUS permite a utilização de um método padronizado para autenticar os usuários na infraestrutura, o que pode ser feito por meio da integração com uma base de dados própria, repositório LDAP (*Lightweight Directory Access Protocol*) ou mesmo o *Active Directory*[7] que esteja conectado à rede. A autenticação é realizada antes de qualquer serviço da rede estar disponível para o usuário. Somente após a autenticação que o usuário tem acesso a serviços como DHCP, DNS e roteamento (RUFINO, 2011).

Os algoritmos referenciados nesta seção serão melhor abordados nos capítulos seguintes.

[7] Active Directory é o serviço de diretórios da Microsoft, utilizado para armazenamento das contas de usuários, autenticação e gerenciamento de permissões.

## 2 RISCOS E AMEAÇAS

Existem diversas questões que podem motivar ataques a redes wireless. É importante que as pessoas e empresas estejam cientes dos riscos e ameaças a que estão expostas ao fazerem uso desta tecnologia. Por mais que essas redes não estejam conectadas a sistemas críticos ou permitam acesso a dados sensíveis, o atacante pode estar simplesmente procurando por um ponto para se conectar a internet.

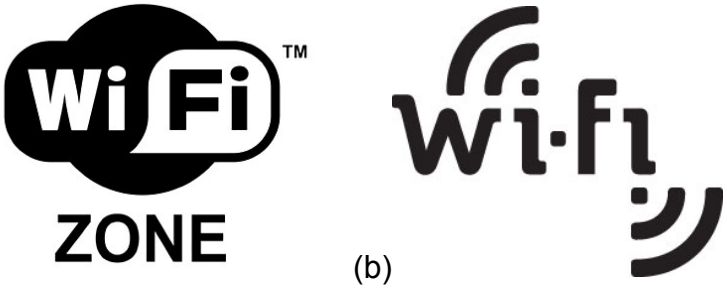
O que a maior parte das pessoas não sabe é que a responsabilidade sob qualquer ato ilícito praticado a partir de um ponto de acesso sem fio recairá sobre o proprietário da rede. No caso de uma investigação criminal as evidências encontradas em servidores e provedores de acesso apontarão para o proprietário da rede, uma vez que as operadoras não monitoram o interior das redes dos clientes. Sua responsabilidade vai até o fornecimento do sinal.

O projeto de lei 2126/2011 conhecido como “Marco Civil da Internet“, determina que empresas que disponibilizem o serviço de acesso a internet, seja gratuitamente ou mediante pagamento, devem identificar e autenticar seus usuários, bem como guardar seus registros de conexão por um período de um ano, sob sigilo em ambiente controlado e de segurança. Determina também que a responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

No caso de uma investigação, o fornecimento das informações de conexão realizadas na rede por um determinado usuário deverá ocorrer somente mediante ordem judicial. Ainda conforme o referido projeto de lei “A violação do dever de sigilo previsto no caput sujeita o infrator às sanções cíveis, criminais e administrativas previstas em lei”.

O disposto no projeto de lei aplica-se não só a provedores de internet e empresas de telecomunicações mas também a qualquer empresa que preste serviço de acesso a internet por meio de rede sem fio. Comuns em aeroportos, centros comerciais, escolas e faculdades, esses pontos de acesso são conhecidos como *hotspots* e comumente identificados por símbolos apresentados na Figura 2. A logomarca “Wi-Fi Zone“ é propriedade da Wi-Fi Alliance para uso em *hotspots* que possuam equipamentos certificados, já a logomarca “Wi-fi Hotspot“ é de irrestrito.

Figura 2 – (a) Logomarca Wi-Fi Zone. (b) Logomarca Wi-Fi Hotspot.




(a) (b)

Fonte – Retirado de https://www.wi-fi.org/media/media-resources.

## 2.1 Taxonomia de ataques de segurança a redes sem fio

Existem diversas tipos de ataques que podem ser aplicados a redes sem fio. Para melhor entendimento das características de cada ataque e possibilidade de agrupamento e classificação de ataques semelhantes, foi proposta uma taxonomia que leva em consideração atributos de cinco aspectos relativos aos ataques (NASR; ABOU EL KALAM; FRABOUL, 2011):

1. **O modo de operação da rede**: infraestrutura ou Ad-Hoc;
2. **Privilégios de acesso:** características de permissão de acesso do atacante (se é um usuário que tem permissão de acesso ou não);
3. **Técnica de ataque:** Pode ser a realização de algum mapeamento ativo ou passivo dos recursos da rede, *spoofing*[8] de IP, MAC ou *frame*[9]. É classificado também quanto a automação (manual, automática ou semiautomática), à taxa (constante, crescente ou intervalada) e por fim quanto a cooperação (ataque autônomo ou cooperativo);
4. **Vulnerabilidade**: relativo a característica da vulnerabilidade explorada. Se foi uma falha na concepção da solução, falha de implementação, configuração ou exposição do meio.
5. **Objetivos**: elevação de privilégios, negação de serviço, comprometimento da integridade dos dados ou extração de dados confidenciais.

[8] *Spoofing* é a técnica em que um elemento malicioso dentro da rede assume a identidade de um elemento, o que Srivatsa (2008) chama de ataque de identidade. Por exemplo, um elemento de rede envia um pacote com o endereço de IP de origem pertencente a outro elemento de rede. Para todos os efeitos, o destinatário assumirá que o pacote teve origem no elemento ao qual o IP pertence. Trata-se de um IP *spoofing*. A mesmá lógica é utilizada para o endereço físico da interface de rede e outras situações.

[9] Refere-se a *Beacon Frame Spoofing*, que consiste na falsificação de pacotes de controle da rede.

As seções seguintes desse capítulo tratam de alguns dos possíveis objetivos de ataques a redes sem fio, com base, em grande parte, no exposto por Howlett (2005).

## 2.2 Interceptação de tráfego

Segundo Howlett (2005, p. 319) "para um *hacker,* a coisa mais fácil é capturar pacotes de uma rede sem fio utilizando um *sniffer*[10]". Esse fato é amplamente documentado e existem diversas ferramentas de código aberto que facilitam essa atividade, mesmo para usuário com pouco conhecimento do funcionamento das dessas redes.

> **Se as ondas de radiofrequência se propagam pelo ar, nada mais normal que estas sejam passiveis de captura**. Caso as informações não estejam devidamente cifradas, não somente o tráfego pode ser copiado, como (e mais grave) seu conteúdo pode ser conhecido (RUFINO, 2011, p.63, grifo nosso).

No parágrafo acima, Rufino observa muito bem a condição intrínseca das redes sem fio e sua consequência em relação a capacidade de interceptação dos dados por terceiros. O autor reforça também a importância de se utilizar métodos de criptografia para proteger o conteúdo das informações trafegadas (tendo em vista a facilidade de interceptação desses dados por dispositivos fisicamente próximos).

O 802.11 prevê mecanismos de criptografia para atacar este problema. Entretanto eles nem sempre são adotados. Pontos de acesso público, pagos ou não, geralmente não adotam a criptografia prevista no 802.11 por questões de simplicidade de uso, tendo em vista que os mecanismos previstos dependem de algum mecanismo de provisionamento anterior ao uso. Por exemplo, a impostação de uma *Pre-Shared Key* (PSK, que é uma senha previamente definida). Isso significa que, em geral, o tráfego dos usuários deste tipo de serviço está "exposto para quem quiser ver". Isso permite, por exemplo, que sejam vistos todos os sites

[10] *Sniffer* é um programa que altera o funcionamento padrão da interface de rede permitindo realizar a captura de todos os pacotes trafegados em um barramento de rede. O comportamento padrão da interface é recuperar somente os pacotes destinados a ela. Esse tipo de ferramenta é muito comum para realizar análise de problemas de funcionamento das redes, bem como auditorias e testes.

pelos quais o usuário está navegando, inclusive o conteúdo que está sendo visualizado pelo usuário, bem como mensagens instantâneas trocadas. Pode permitir também a captura de senhas e credenciais de acesso, inclusive em redes que utilizam como forma de proteção o padrão WEP. Conforme será visto nas seções seguintes, a chave de criptográfica utilizada para prover confidencialidade dos dados é compartilhada por todos os usuários da rede, o que permite que qualquer trafego seja decifrado (HOWLETT, 2005). Afora outras vulnerabilidades descobertas no protocolo que facilitam a quebra da chave de criptografia, tornando-o incapaz de efetivamente agregar segurança a uma rede.

É claro que não se pode generalizar. Existem mecanismos para resolver esse problema em camadas de rede acima do 802.11, como, por exemplo, o uso de VPN (*Virtual Private Network*) que é a melhor solução existente hoje. Outra solução é o uso de SSL diretamente pelas aplicações, a exemplo do HTTPS adotado por muitos serviços na internet como bancos, provedores de e-mail e redes sociais como o Facebook (a maior e mais popular atualmente). Entretanto, vale reforçar que essa solução atua de forma pontual, cifrando apenas o conteúdo de cada site que faz uso dela, de forma individual.

Para redes não públicas é muito importante observar o posicionamento dos equipamentos para evitar o “vazamento” de sinal para fora do perímetro físico em que se deseja que a rede esteja disponível. “Deve-se lembrar que, mesmo que o sinal seja fraco fora do ambiente desejado, equipamentos com melhor recepção podem fazer uso dele“ (RUFINO, 2011, p. 47).

## 2.3 Acesso a computadores com tecnologia de rede sem fio

Para um atacante, dispositivos com capacidades de uso de redes sem fio são vetores de acesso a máquinas dentro de uma rede. Em algumas situações, é possível enxergar de fora computadores ligados a uma rede sem fio. Essa máquina torna-se, então, alvo de um atacante que pode ter o objetivo de tomar o controle da máquina para então ter um ponto de entrada na rede. Além do mais, essa máquina

provavelmente não estará protegida por um *firewall*[11] e nem terá os mesmos recursos de proteção utilizados no perímetro da rede ou em servidores (HOWLETT, 2005). Essas alterações da topologia da rede trazem também a necessidade de rever o posicionamento dos elementos de segurança.

## 2.4 Acesso a rede local

Howlett (2005, p. 319) aponta esse como o provável maior perigo representado pelas redes sem fio. O autor faz um analogia em que compara o fato de um *hacker* conseguir acesso a uma determinada rede local a possuir as “chaves do reinado”. O que o autor quer dizer é que a partir da rede o *hacker* poderá conseguir um IP válido e então começar a explorar a rede, buscando descobrir novos serviços e elementos para dominar. O autor ressalta também a capacidade de utilização de *scanners*[12] de vulnerabilidades e portas a exemplo do Nessus e Nmap, afim de encontrar brechas que possam ser exploradas.

## 2.5 Acesso anônimo a internet

Conforme citado na seção introdutória deste capítulo, um atacante pode acessar uma rede sem fio sem estar particularmente interessado em algum elemento ou dado presente naquela rede. O objetivo pode ser simplesmente conseguir um ponto de acesso a internet para execução de atividades ilícitas de forma anônima, sem deixar rastros, uma vez que qualquer evidência levará a rede utilizada e não ao usuário. Além do mais a chance de pegar alguém que esteja realizando um acesso por meio de uma rede sem fio é muito pequeno, a não ser que se tenha equipamentos previamente disponíveis no local para realização de

[11] Firewall é um elemento de segurança de rede especializado em controle de fluxo de entrada e saída de dados. É utilizado para dividir dois segmentos de rede, de modo a controlar todo o tráfego de um segmento para o outro, permitindo ou não sua passagem. A abordagem da grande maioria destes elementos nega a passagem de qualquer tráfego a não ser que ele seja explicitamente permitido por meio da impostação de uma regra. Regras de *firewall* geralmente levam em consideração os endereços IP de origem e destino, o tipo de transporte (TCP/UDP) e as portas utilizadas.

[12] *Scanners* são programas para realização de varreduras.

triangulação de sinal. “Redes sem fio inseguras oferecem aos hackers a melhor forma de acesso anônimo que existe“ (HOWLETT, 2005, p. 319).

## 2.6 Negação de serviço

Uma das modalidades de ataque mais relegadas pelos administradores de rede segundo Rufino (2011). O autor afirma que a maior preocupação dos administradores de rede se volta para o controle de acesso e proteção da privacidade dos dados dos usuários e que muitas vezes ataques de negação de serviço nem sequer são incluídos no mapa de risco.

Esse tipo de ataque é mais direcionado para a camada física, com a geração de sinais de rádio que causem interferência no sinal da rede. Conhecidos como ataques de DOS (do inglês Denial of Service), em se tratando de redes sem fio, podem ser direcionados a concentradores e conexões ou a dispositivos causando indisponibilidade do serviço ou diminuição drástica da capacidade de atendimento.

Dispositivos móveis geralmente possuem recursos limitados, tornando-os mais susceptíveis a interferências geradas por adversários com maior potência de sinal (SRIVATSA, 2008).

Conforme citado no capítulo um, as redes sofrem também interferência de outros dispositivos em uso legítimo que podem acarretar na diminuição da qualidade do serviço, como é o caso dos dispositivos Bluetooth.

Farooq, Llewellyn-Jones e Merabti (2010) descrevem um tipo de ataque de negação de serviço realizado na camada MAC do 802.11. Nessa variante o atacante forja o endereço MAC de um dispositivo da rede (MAC *spoofing*), assumindo sua identidade e interrompendo o funcionamento da rede. Os autores explicam que esse ataque é possível pelo fato do 802.11 não prover mecanismos para autenticação de origem dos pacotes, o que viabiliza o MAC *spoofing*.

Um caso interessante evidenciado por Rufino (2011, p. 47) é que “basta existir um dispositivo 802.11b em uma rede 802.11g para uma queda geral de performance (velocidade)”. Nesse caso pode se tratar de um uso legítimo de um

dispositivo 802.11b que, pelo fato das redes “g” manterem compatibilidade com o padrão “b”, alteram seu comportamento para funcionar no padrão mais antigo, com menores taxas de transferência. Entretanto, sempre existe a possibilidade de um atacante deliberadamente associar um dispositivo “b” a rede para provocar uma queda de performance.

## 2.7 Vulnerabilidades específicas do 802.11

As redes sem fio possuem diversas vulnerabilidades que são intrínsecas, ou seja, relacionadas a características que são destas redes que não podem ser alteradas, como a transmissão pelo ar. Entretanto, diversas outras vulnerabilidades são específicas do padrão 802.11. Algumas delas decorrentes de implementações ou configurações ruins realizadas por alguns fabricantes, outras decorrentes de problemas de concepção e projeto do 802.11 (HOWLETT, 2005).

Segundo Howlett (2005) algumas delas são:

- **Uso de SSIDs padrão**: pode ser um indício de que não foi dada muita atenção para a configuração da rede, não sendo raro encontrar equipamentos com muitas configurações de fábrica (geralmente com baixa segurança). Além disso, essa característica possibilita emprego *rainbow tables*[13] em ataques de força bruta para obtenção da PKS (*Pre-Shared Key*) no WPA e WPA2;
- **Divulgação da existência da rede**: por padrão as redes Wi-Fi anunciam constantemente sua existência a potenciais usuários – o que é chamado de *Beacon*[14] *Broadcast*[15]*.* A partir desse sinal usuários podem descobrir a rede e negociar a abertura de uma sessão. Um dos problemas é que este sinal é transmitido em claro, pois os usuários ainda não estão autenticados, e portanto pode ser capturado. Isso faz

[13] Uma *rainbow table* é, essencialmente, uma tabela pré-calculada de funções hash de um conjunto determinado de entradas para possibilitar sua função inversa. Normalmente utilizadas para “quebrar” hashes de senhas. Essas tabelas são normalmente utilizadas para se recuperar uma senha a partir de seu hash até um dado limite de comprimento da senha e conjunto de caracteres possíveis (GOLD, 2011).
[14] *Beacon* é um tipo de pacote de controle das redes sem fio. Normalmente utilizado para divulgar sua existência.
[15] Broadcast é a difusão aberta de um determinado conteúdo para todos os elementos em um raio de alcance, a exemplo do que acontece com o sinal da televisão aberta.

com que qualquer cliente saiba da existência da sua rede. Uma abordagem recomendada é desabilitar essa característica. Isso dificulta o descobrimento da existência da rede e evita a divulgação do SSID que faz parte do protocolo de segurança para autenticação. Entretanto, é importante ressaltar que estes benefícios existem somente enquanto não há dispositivo utilizando a rede pois todas estas informações podem ser obtidas a partir da escuta do tráfego;

- **Transmissões em claro por padrão**: a maioria dos fabricantes adota configurações de transmissão em claro por padrão em seus equipamentos, deixando a cargo do administrador fazer as alterações necessárias para ativar os protocolos de segurança. Isso se torna um problema maior para usuários domésticos que podem não dominar os conhecimentos necessários para realizar os ajustes de configuração;
- **Fragilidade do protocolo WEP**: por questões de compatibilidade com dispositivos mais antigos, a maioria dos fabricantes ainda mantém disponível para uso o protocolo WEP, cujas vulnerabilidades encontram-se amplamente divulgadas. Fica a cargo do administrador fazer o uso da tecnologia ou não. Novamente pode ser um problema no caso de usuários domésticos.

# 3 PROTOCOLOS DE SEGURANÇA

A partir das informações apresentadas até o momento, é possível compreender em parte o papel da segurança e sua importância para a difusão do uso das redes sem fio, principalmente em se tratando de ambientes corporativos onde o vazamento de informações pode acarretar em significativos prejuízos financeiros.

Este capítulo apresenta um pouco do funcionamento dos principais protocolos de segurança presentes no padrão 802.11, evidenciando seus objetivos e falhas conhecidas. O objetivo deste trabalho não é explorar todas as características e vulnerabilidades dos protocolos de forma exaustiva. A intenção é dar uma visão geral dos problemas, sendo que muitos deles poderão ser observados a partir dos dados coletados no estudo de caso.

## 3.1 Segurança da informação

Antes de detalhar o funcionamento dos protocolos de segurança é preciso entender melhor seus objetivos de uma forma geral. Para isso, serão utilizados alguns conceitos citados ou definidos segundo a norma ABNT NBR ISO/IEC 27001:2006 que trata de técnicas de segurança, sistemas de gestão de segurança e requisitos em tecnologia da informação.

Nesse contexto, pode-se considerar as redes de computadores, e mais especificamente as redes sem fio, como parte de um sistema de tecnologia da informação. Sendo assim, as definições presentes na norma aplicam-se as redes sem fio.

A norma define **segurança da informação** como “preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como, autenticidade, responsabilidade, não repúdio e confiabilidade, podem estar envolvidas” (ABNT NBR ISO/IEC 17799:2005 apud ABNT NBR ISO/IEC 27001:2006, p. 2, grifo nosso). É possível identificar claramente que a finalidade dos protocolos está relacionada ao conceito.

O conceito de **confidencialidade** apresentado na norma é a “propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados” (ISO/IEC 13335-1:2004 apud ABNT NBR ISO/IEC 27001:2006, p. 2, grifo nosso). O que é automaticamente associado a uma das vulnerabilidades intrínsecas das redes sem fio, o meio, conforme tratado no capítulo anterior. Como a comunicação pode ser capturada por alguém não autorizado a acessar os dados, é preciso garantir seu sigilo por meio do uso de algoritmos fortes de criptografia. Desse modo, a comunicação pode ser capturada, porém não será possível acessar os dados que foram trafegados.

Neste mesmo contexto, é necessária a manutenção da **integridade** das informações, definida como a “propriedade de salvaguarda da exatidão e completeza de ativos“ (ISO/IEC 13335-1:2004 apud ABNT NBR ISO/IEC 27001:2006, p. 3, grifo nosso), onde considera-se ativo “qualquer coisa que tenha valor para a organização”. Aqui, está se falando dos dados trafegados na rede. É preciso garantir que a comunicação não seja adulterada.

Com relação a **disponibilidade**, definida como a “propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada“ (ISO/IEC 13335-1:2004 apud ABNT NBR ISO/IEC 27001:2006, p. 2), o capítulo dois aborda como os ataques de negação de serviço visam comprometer essa propriedade da rede, enfatizado como os mecanismos de funcionamento da rede podem facilitar ou dificultar esses ataques.

Conforme visto nos parágrafos anteriores, tanto as definições de confidencialidade quanto disponibilidade, levam em consideração a entidade que está acessando os dados. Ambas as definições deixam claro que a entidade deve ter autorização, o que nos remete a mecanismos para realização de controle de acesso. No casos das redes sem fio, pode ser realizado o controle de acesso tanto dos dispositivos, quanto dos indivíduos autorizados a fazer uso da rede.

A realização do controle de acesso não existe sem o apoio de mecanismos de identificação e autenticação[16], que também são tópicos cobertos pelos protocolos de segurança do 802.11.

[16] Em segurança da informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema.

Qualquer evento que ameace a segurança da informação é chamado de **incidente de segurança da informação**. É definido formalmente como “um simples ou uma série de eventos de segurança da informação[17] indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação” (ISO/IEC TR 18044:2004 apud ABNT NBR ISO/IEC 27001:2006, p. 2).

Tem-se então, que o objetivo dos protocolos de segurança do 802.11 é garantir a confidencialidade, integridade e disponibilidade (ora chamados de objetivos de segurança) das redes e dos dados trafegados por elas, de modo a evitar da melhor maneira possível a ocorrência de incidentes de segurança da informação.

## 3.2 Os protocolos de segurança do 802.11

Conforme abordado no capítulo um, são vários os protocolos necessários para garantir objetivos de segurança de confidencialidade, integridade e disponibilidade. Ao longo dos anos, alguns deles mostraram-se pouco eficientes, havendo a descoberta de diversas falhas e problemas em sua concepção.

Nisbet (2012) observa muito bem o fato de que a segurança de qualquer rede deve ser construída em diversas camadas, de forma que tentativas de invasão tenham que superar mais de um obstáculo para que tenham sucesso.

Os principais protocolos de segurança do 802.11 atuam na camada de enlace do modelo OSI. Sendo que, existem três grandes abordagens de segurança trazidas por gerações diferentes de protocolos (LASHKARI; DANESH; SAMADI, 2009). São eles:

- WEP (*Wired Equivalent Privacy*)
- WPA (Wi-Fi *Protected Access*)
- WPA2/802.11i (Wi-Fi *Protection Access*, Versão 2)

[17] Evento de segurança da informação é “uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação“ (ISO/IEC TD 18044:2004 apud ABNT NBR ISO/IEC 27001:2006, p. 2).

O quadro 2 compara as principais características de cada um destes protocolos, detalhados nas seções seguintes.

Quadro 1 - Comparativo WEP, WPA e WPA2.

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Cifra** | RC4 | RC4 | AES |
| **Tamanho da chave** | 40 bits | 128 bits | 128 bits |
| **Tempo de vida da chave*** | IV de 24bits | IV de 48bits | IV de 48bits |
| **Chave do pacote** | Concatenada | *Temporal Key Hash* | (Não necessária) |
| **Integridade dos dados** | CRC-32 | Michael | CCM |
| **Integridade do cabeçalho** | Não | Michael | CCM |
| **Mitiga ataque de *replay*[18]** | Não | Controle de sequência de IV | Controle de sequência de IV |
| **Gerenciamento de chaves** | Não | Com uso do EAP | Com uso do EAP |

Fonte – Adaptado de Nisbet (2012).
*O tempo de vida da chave está associado a quantidade de IVs (vetores de inicialização) possíveis, uma vez que o mesmo vetor de inicialização não deve ser reutilizado (BORISOV; GOLDBERG; WAGNER, 2001). Diversos autores alertam para esse perigo, pois ataques para quebra da chave utilizam essa falha. É o caso dos ataques realizados no WEP.

## 3.3 802.11 Wired Equivalent Privacy (WEP)

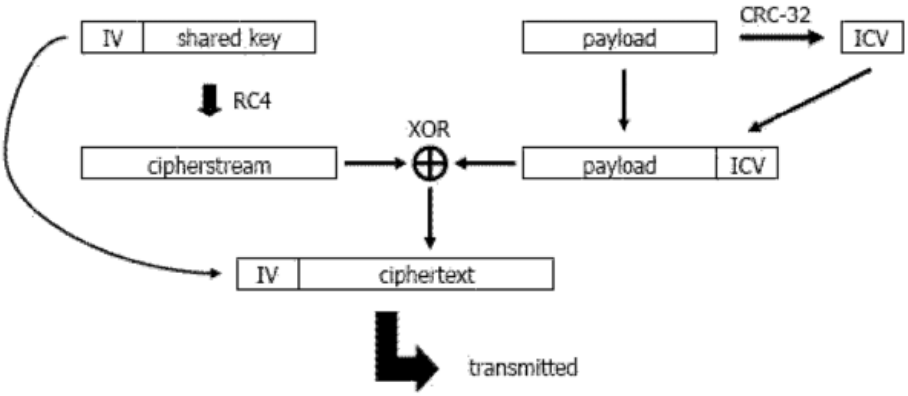
O padrão 802.11 publicado em 1999 inclui a especificação do protocolo de segurança chamado *Wired Equivalent Privacy*, que como o nome diz, tinha como objetivo prover um nível de segurança equivalente ao das redes cabeadas do padrão Ethernet. Ele deveria garantir a confidencialidade e integridade dos pacotes da rede (MOEN; RADDUM; HOLE, 2004).

O WEP utiliza a cifra de fluxo RC4 para prover confidencialidade, com uso de chaves de 40bits (na versão inicial), concatenadas a um vetor de inicialização (IV) de 24bits, que é transmitido em claro, totalizando uma chave de 64bits. Essa chave é utilizada como entrada para o RC4 para produzir o *keystream*[19]. O transmissor realiza a operação XOR entre o "texto puro"[20] e o *keystream* para obtenção do texto cifrado, conforme diagrama 1 (GURKAS; ZAIM; AYDIN, 2006).

[18] No ataque de *replay* pacotes transmitidos na rede são capturados, armazenados e retransmitidos como um novo pacote válido, sem a necessidade de alterações no pacote.
[19] Em criptografia o *keystream* é um fluxo de caracteres pseudorrandômicos que são combinados com o "texto puro", dando origem ao texto cifrado (MENEZES; OORSCHOT; VANSTONE, 2001).
[20] "Texto puro" ou "texto plano" é a denominação dada aos dados em claro, que não estejam criptografados.

O algoritmo *Cyclic Redundancy Check* (CRC-32) é utilizado para calcular o ICV (*Integrity Check Value*), que vai anexado à mensagem antes que esta seja cifrada utilizando o RC4 (MOEN; RADDUM; HOLE, 2004). Como o nome diz, tem o objetivo de prover um método de verificação da integridade da mensagem. O destinatário da mensagem realiza o procedimento inverso, realizando a checagem de integridade com o CRC-32.

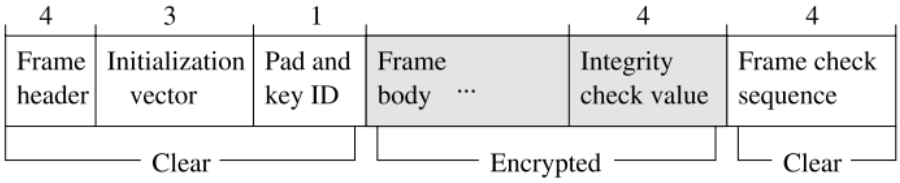
Diagrama 1 – Fluxo de execução do WEP




Fonte – Gurkas, Zaim e Aydin (2006).

O tamanho original das chaves do WEP se deve a uma restrição de exportação de criptografia com chaves maiores do que 64bits, existente à época nos Estados Unidos (RUFINO, 2011). Posteriormente foi adicionada a capacidade de trabalhar com chaves de 104bits e até chaves maiores em implementações de alguns fabricantes. A figura 3 mostra o formato de um pacote WEP.

Figura 3 – Pacote WEP com comprimentos de campos em bytes.




Fonte – Moen, Raddum e Hole (2004).

### 3.3.1 *Vulnerabilidades conhecidas do WEP*

Já foi demonstrado que o WEP tem diversas falhas de projeto, de modo que não é capaz de cumprir os objetivos para os quais foi projetado. Dentre os

problemas encontrados no WEP, ficou evidente que ele não é capaz de proteger a rede contra pacotes forjados e ataques de replay, permitindo que um atacante utilize a própria infraestrutura da rede para lançar ataques que permitam a recuperação da chave de criptografia do WEP (MOEN; RADDUM; HOLE, 2004).

O CRC-32 utilizado para o cálculo do ICV possui grande probabilidade de detectar alterações em um único bit do pacote, entretanto, não é seguro do ponto de vista criptográfico (MOEN; RADDUM; HOLE, 2004). Borisov, Goldberg e Wagner (2001) demonstraram que é possível realizar modificações em uma mensagem cifrada sem invalidar o ICV.

Já em 2004 a ferramenta AirSnort era capaz de decifrar os dados trafegados em redes sem fio que utilizavam WEP, fato que é atribuído a forma como o WEP faz uso do protocolo RC4 (MOEN; RADDUM; HOLE, 2004), apenas concatenando a chave a um IV que é enviado em claro (conforme ilustrado na figura 3). Estudos recentes apresentam ataques ao algoritmo RC4 que permitem a quebra da confidencialidade dos dados independentemente da implementação do WEP (ALFARDAN et al., 2013). Hoje este protocolo é considerado depreciado e portanto seu uso não é recomendado.

Outro ponto frágil do WEP reside no fato de que todos os dispositivos conectados a um AP compartilham a mesma PSK, o que lhes confere a capacidade de decifrar qualquer pacote trafegado. Além do mais, não existe qualquer mecanismo de gerenciamento das chaves, que são distribuídas manualmente entre os dispositivos. Consequentemente, é pouco provável que ela seja alterada com frequência.

Um dos problemas mais graves é o fato do IV ser muito pequeno, apenas 24bits. Isso implica que fatalmente haverá reuso dos IVs, o que é conhecido como "*two-time pad*" (BORISOV; GOLDBERG; WAGNER, 2001). É apenas uma questão de tempo, associada ao volume de trafego da rede.

Esse problema é agravado pelo fato de que o WEP não realiza verificação de sequencial dos IVs utilizados, possibilitando a realização de reenvio de um pacote capturado na rede (*replay*). Um ataque chamado APR *Request Replay* aproveita-se dessa característica para aumentar artificialmente o tráfego da rede e capturar IVs com o objetivo de quebrar recuperar a PSK. Esse processo pode ser realizado com a ferramenta de código aberto airreplay-ng, parte da suíte aircrack-ng.

Gold (2011) afirma que com a potência presente nos equipamentos domésticos atuais é possível quebrar uma chave WEP em menos de 30 segundos.

Um ataque que explora o WEP e tem por objetivo quebrar a confidencialidade da comunicação sem necessariamente quebrar o chave de criptografia é o Chop-Chop (RUFINO, 2011). Seu modelo matemático é dado por Guennoun et al. (2008).

Rufino (2011) aponta também problemas relativos a implementação do WEP, como por exemplo a guarda da PSK nos dispositivos que é realizada em claro. Pode ser mais fácil recuperar a chave a partir do dispositivo do que realizar um ataque de força bruta na rede. O autor expõe também que muitos equipamentos utilizam sempre a mesma sequencia de IV, a partir do momento em que são ligados. O que caracteriza o "*two-time pad"* visto que a chave do WEP nunca muda.

Lashkari, Danesh e Samadi (2009) resumem os problemas encontrados no WEP aos seguintes:

- Não previne a falsificação de pacotes;
- Não previne ataques de *replay*, permitindo a um atacante simplesmente gravar e reenviar pacotes a sua vontade de modo que estes pacotes serão aceitos como legítimos;
- Usa o RC4 de maneira inadequada, pois as chaves são fracas[21] o que possibilita a realização de força bruta em poucos minutos, com programas distribuídos gratuitamente;
- Reuso de vetores de inicialização (IVs). Diversos métodos de criptoanálise disponíveis hoje conseguem decifrar dados sem necessitar de saber a chave de criptografia;
- Permite a um atacante modificar uma mensagem sem precisar saber a chave de criptografia e sem ser detectado;
- Não possui gerenciamento de chaves o que torna difícil sua atualização e distribuição;
- O algoritmo RC4 possui problemas;
- Facilidade de falsificação de mensagens de autenticação.

[21] Hoje o WEP é considerado inseguro para qualquer tamanho de chave. Fato apontado por Walker et al. (2000).

Podemos adicionar ainda os problemas de implementação existentes conforme Rufino (2011):

- Muitos equipamentos utilizam o mesmo sequencial de IVs a partir do momento em que são ligados;
- Clientes armazenam as chaves em claro;

Rufino (2011, p. 71) relata que “apesar de não fazer parte do WEP padrão, alguns fabricantes implementam a troca dinâmica de chaves como forma de tentar evitar a quebra da chave, já que ela pode variar por um tempo não suficiente para que a chave seja quebrada”. O autor finaliza com a seguinte colocação: “Vários são os métodos para explorar vulnerabilidades do WEP; atualmente não existe nenhuma razão para usar uma tecnologia tão frágil como essa”.

### 3.4 Wi-fi Protected Access (WPA)

O WPA é uma especificação de segurança desenhada para ser interoperável. Foi projetada para manter compatibilidade com o hardware existente à época, de modo que sua implantação dependesse apenas de atualizações de *software* ou *firmware* (WONG, 2003).

O padrão é baseado em um subconjunto do padrão 802.11i (até então em desenvolvimento) que agregou três principais melhorias de segurança ao 802.11:

- Implementou autenticação baseada no 802.1x e no EAP, possibilitando a realização de autenticação mútua entre dispositivos/usuários e AP;
- Aplica o protocolo TKIP (*Temporal Key Integrity Protocol*) ao RC4 (encapsulado no WEP) para melhorar a qualidade da criptografia (é importante ressaltar que o RC4 é mantido apenas por questões de compatibilidade com *hardware* legado);
- Utiliza o protocolo Michael verificação de integridade das mensagens.

Foi concebido como uma solução de caráter imediato e temporário, considerado um “tapa buraco” criado para mitigar as vulnerabilidades existentes no WEP. Foi pensado para ter compatibilidade com o 802.11i quando este fosse aprovado, visto que todos os produtos devem estar aderentes ao padrão uma vez que é liberado (WONG, 2003).

O WPA possui dois modos de operação, o WAP Pessoal ou WPA-PSK (de Pre-Shared Key, o que significa que existe uma chave de autenticação compartilhada por todos os usuários) e o WPA Empresarial.

O primeiro foi pensado para uso domestico e em pequenas empresas. É mais simples de instalar pois não necessita de um servidor de autenticação. Sua chave de criptografia pode ser de até 256bits.

No segundo método é necessário o uso de um servidor de autenticação 802.1x, o que permite uma autenticação mais granular, feita especificamente para cada usuário. Nesse modo de operação não existe PSK (LASHKARI; DANESH; SAMADI, 2009).

### 3.4.1 802.1x baseado no *Extensible Authentication Protocol (EAP)*

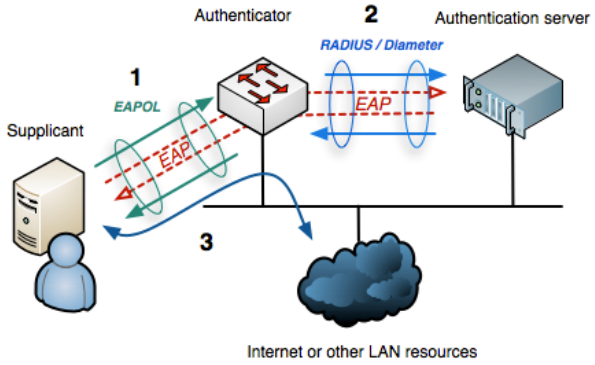
O padrão 802.1x foi adicionado ao WPA para possibilitar a autenticação de usuário (inexistente no WEP). Esse padrão foi projetado para uso inicialmente em redes cabeadas, entretanto, é compatível com o uso em redes sem fio. O padrão permite controle de acesso baseado em portas, bem como autenticação mútua entre clientes e APs por meio de um servidor de autenticação (WONG, 2003).

Para que uma porta de comunicação seja utilizada, primeiro o cliente (chamado suplicante pelo 802.1x) deve se autenticar. Até que o cliente esteja autenticado nenhum tráfego é permitido. Todo o tráfego, incluindo os protocolos DHCP, HTTP, FTP, SMTP e POP3 são bloqueados. A única exceção é o tráfego específico do 802.1x (WONG, 2003).

O EAP é o protocolo utilizado pelo 802.1x para realizar o processo de autenticação. Ele provê uma camada de abstração para a rede sem fio, permitindo que seja escolhido um sistema específico de autenticação a ser utilizado, podendo-

se utilizar senhas, certificados digitais ou mesmo *tokens* OTP[22] e similares. Com o EAP o autenticador não necessita de conhecer o funcionamento dos métodos de autenticação, agindo como um intermediário que encapsula as mensagens do EAP que são transmitidas entre o suplicante e o servidor de autenticação (WONG, 2003), conforme ilustrado na figura 4.

Figura 4 – 802.1x.




Fonte – Wikipedia, disponível em <http://en.wikipedia.org/wiki/IEEE_802.1X>. Acessado em 27 de out. de 2013.

### 3.4.2 *Temporal Key Integrity Protocol (TKIP)*

Projetado pelo grupo de trabalho do IEEE 802.11i em conjunto com a Wi-Fi Alliance, o TKIP encapsula o WEP. É o responsável por grande parte das melhorias de segurança, mantendo a premissa de ser compatível com o hardware legado. Foi depreciado em janeiro de 2009 pelo IEEE.

As melhorias introduzidas pelo TKIP podem se resumir a quatro itens (LASHKARI; DANESH; SAMADI, 2009):

- Adoção de um MIC (*Message Integrity Code*) baseado em criptografia para impedir falsificações de pacotes (trata-se do algoritmo Michael citado anteriormente);
- Implantação de uma metodologia para verificação de sequencial dos IVs, do modo a combater os ataques de *replay*;

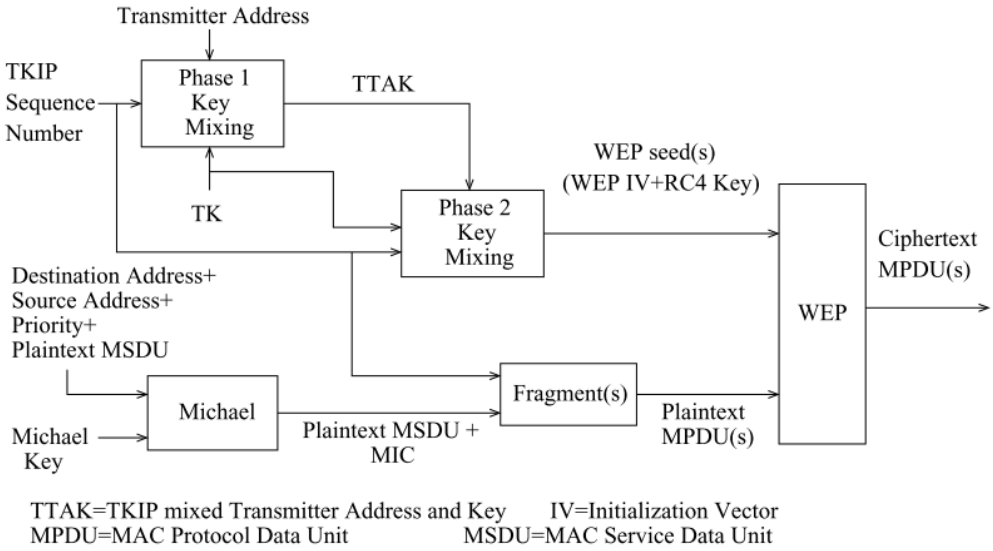
[22] OTP é a sigla para One-Time Password. Consiste em um sistema para uso de senhas descartáveis, válidas somente para uma iteração de autenticação. A RFC 2289 descreve este mecanismo.

- A utilização de uma função de embaralhamento de chaves, aplicada por pacote, para diminuir a correlação entre IV que é publico e uma chave;
- Utilização de uma mecanismo de *rekeying,* que é a geração de novas chaves de sessão[23] periodicamente, buscando evitar ataques decorrentes do reuso de chaves.

Para garantir que cada cliente conectado a rede utilize chaves de criptografia diferentes, estas são geradas com base em uma chave temporal de 128bits (compartilhada entre cliente e AP), o endereço MAC do dispositivo cliente e um IV de 48bits, que está relacionado ao número sequencial dos pacotes.

Para o processo de cifra (ilustrado no diagrama 2) do TKIP uma chave temporária (TK – *Temporal Key*), obtida do sistema de gerenciamento de chaves durante o processo de autenticação, é passada como entrada para a função *Temporal Key Hash* (representada no diagrama 2 pela fase 1 e 2 do processo denominado *Key Mixing*) em conjunto com o endereço do transmissor de 6bytes (TA – *Transmitter Address*) e o vetor de inicialização (IV) de 48bits, também chamado de "contador sequencial do TKIP" (MOEN; RADDUM; HOLE, 2004).

Diagrama 2 – Fluxo de cifração do algoritmo TKIP.




Fonte – Huang et al. (2005).

[23] Chave de sessão é a chave de criptografia utilizada em um comunicação em andamento.

A função de *hash* gera uma saída de 16-bytes que será a chave do RC4, sendo os primeiros bytes derivados do IV. Essa chave é usada em apenas um pacote WEP, visto que os IVs funcionam como um contador sequencial que aumenta a cada pacote. Por isso, essa chave é conhecida como per-packet key (ou chave do pacote). Esse processo diminui a quantidade de dados cifrados com a mesma chave e ao mesmo tempo mitiga ataques de replay dado que o receptor não deve aceitar pacotes com o IV menor ou igual ao de um pacote recebido anteriormente (MOEN; RADDUM; HOLE, 2004).

A integridade da mensagem é garantida pelo MIC (*Message Integrity Code*). O TKIP utiliza o algoritmo Michael para sua geração, conforme descrito na seção seguinte.

### 3.4.3 *Michael Message Integrity Check*

*Message Integrity Code* (MIC) é o nome genérico dado ao produto de uma função utilizada para verificação da integridade de mensagens. Michael é o nome do algoritmo utilizado para calcular o MIC de 64bits utilizado pelo TKIP. Seu propósito é identificar alterações nos pacotes transmitidos na rede, sejam elas ocasionadas por erros na transmissão ou por manipulação intencional (WONG, 2003).

Michael é uma função *hash* assinada eletronicamente com uma chave criptográfica. Recebe como entrada uma chave de 64bits, denominada "*Michael Key*" e uma mensagem de tamanho qualquer (HUANG et al., 2005).

Conforme pode ser observado no diagrama 2, no TKIP o algoritmo Michael recebe como entrada os seguintes parâmetros concatenados: endereço de destino (*Destination Address*+), endereço de origem (*Source Address*+), a prioridade do pacote (*Priority*+), a mensagem a ser transmitida (*Plaintext* MSDU) e por fim a chave criptográfica (*Michael Key*). Os campos marcado com o sinal de mais (+) fazem parte do cabeçalho do pacote, permitindo que alterações sejam detectadas (HUANG et al., 2005).

O MIC resultante do cálculo realizado pelo algoritmo Michael é então concatenado a mensagem a ser transmitida (*Plaintext* MSDU) que, dependendo de

seu tamanho pode ser fragmentada para a geração do *Plaintext* MPDU. Só então, o MPDU é repassado como entrada do algoritmo WEP, que realizará a codificação dos dados utilizando o algoritmo RC4 (MOEN; RADDUM; HOLE, 2004).

### 3.4.4 *Vulnerabilidades conhecidas do WPA*

Apesar de melhorar muitos aspectos da segurança em relação ao WEP, existem diversas vulnerabilidades documentadas, presentes nos algoritmos utilizados no WPA.

Com relação ao algoritmo *Temporal Key Hash,* Moen, Raddum e Hole (2004) fazem uma análise em que demonstram a possibilidade de recuperação das chaves usadas para criptografia dos pacotes. Esse problema pode parecer menos relevante se pensarmos que cada pacote é cifrado com uma chave diferente, entretanto, os autores demonstram também que com algumas chaves de pacote recuperadas é possível obter a chave de sessão (*Temporal Key*). Como consequência, o atacante conseguiria decifrar todo o trafego da sessão. Os autores afirmam ainda que o WPA não emprega o conceito de "*perfect forward secrecy*"[24], uma vez que de posse de algumas chaves de pacote é possível calcular chaves anteriores e futuras.

Já o algoritmo Michael, fundamental para evitar alterações nos dados trafegados, e por isso, também é parte fundamental na mitigação de ataques de *replay* é analisado por Huang et al., (2005). Dentre as vulnerabilidades encontradas no algoritmo destaca-se o fato dele não ser uma função *one-way*, ou seja, a partir de resultado é possível derivar os parâmetros de entrada. Fato grave, pois expõe a chave denominada *Michael Key*, o que sujeita o algoritmo a problemas semelhantes aos enfrentados pelo WEP com o uso do CRC-32, como a capacidade de um atacante alterar o conteúdo dos pacotes enviados. O outro grande problema é a possibilidade de colisão do algoritmo. Isso implica que um atacante teria certa "facilidade" em produzir mensagens que gerassem o mesmo MIC.

---

[24] *Perfect Forward Secrecy* é a propriedade dos protocolos de troca de chaves que garante que chaves de sessão derivadas de um conjunto de chaves de longo prazo (tanto públicas quanto privadas) não sejam comprometidas caso algumas das chaves de longo prazo venha a ser.

Um dos ataques mais comuns ao WPA está relacionado ao processo de autenticação em redes WPA-PSK, mais especificamente, ao processo de autenticação denominado *4-way handshake* pois ocorre em quatro etapas correspondentes a uma mensagem cada, trocas entre cliente e AP. Moskowits (2003) explica como obter a PSK da rede a partir da captura do *4-way handshake* no qual é realizado um ataque de dicionário ou força bruta. Esse ataque pode ser realizado *off-line*, ou seja, não depende da infraestrutura da rede. Uma vez capturados os dados de autenticação a força bruta pode ser realizada em qualquer computador.

Conforme Gold (2011), o pesquisador de segurança Moxie Marlinspike lançou, em 2009, um serviço on-line que se aproveita dessa vulnerabilidade para quebrar o *4-way handshake* e obter a *Pre-Shared Keys*. Lançado sob o domínio WPAcracker.com, o serviço era oferecido por um valor de $17,00 (dezessete dólares americanos) por PSK a ser quebrada. Pra cumprir a tarefa, o serviço utiliza-se de computação paralela. Originalmente com um cluster de 400 máquinas, era capaz de testar 130 milhões de combinação em 20 minutos. Hoje, hospedado no domínio cloidcracker.com, é capaz de testar 300 milhões de combinações no mesmo intervalo de tempo. Atualmente existem diversos softwares para fazer isso, entretanto, o diferencial do serviço consiste em seu grande poder computacional. O autor aponta ainda que a forma de mitigar esse tipo de ataque é utilizar senhas grandes, de no mínimo 20 caracteres ou mais, combinando letras, número e caracteres especiais.

Em relação ao RC4, conforme citado nas seções anteriores, estudos apontam o algoritmo como quebrado, e portanto não recomendado para uso (ALFARDAN et al., 2013).

Rufino (2011) aponta ainda a possibilidade de aplicação de um uma variante do ataque chop-chop, utilizado no WEP. Alerta também para problemas de implementação relativos ao armazenamento de chaves em claro nos clientes e concentradores, o que fragiliza o processo da segurança como um todo.

### 3.5 802.11i/Wi-fi Protected Access2 (WPA2)

WPA2 é o nome comercial relacionado a implementação do padrão 802.11i, um padrão de segurança projetado para ser durável. Dentre as alterações realizadas, a escolha do AES como padrão de criptografia é apontada como umas das mais importantes. Definido pelo NIST (*National Instiure of Standards and Technology*) como o sucessor robusto para DES (Data Encription Standard) em outubro de 2000 (LASHKARI; DANESH; SAMADI, 2009). Embora acredite-se que o AES seja um algoritmo de criptográfico, muitas pessoas não sabem que ele é um padrão definido pelo NIST que faz uso do algoritmo criptográfico Rijndael. Quando se fala em AES, significa que se está utilizando o Rijndael com uma chave de 128bits e bloco de mesmo tamanho.

Alguns dos motivos para a escolha do AES são a vasta documentação, o fato de ser livre de patentes ou *royalties* e o fato de ter sido submetido a extensivo trabalho de revisão pública. Essa mudança também significou a necessidade de atualização do *hardware* (LASHKARI; DANESH; SAMADI, 2009).

Além do AES destacam-se dentre as funcionalidades trazidas pelo WPA2 os seguintes métodos de criptografia:

- TKIP – Mantido para manter compatibilidade dispositivos legados, e funciona da mesma maneira que no WPA. Traz também os mesmo problemas e por isso foi depreciado em 2009 pelo IEEE, não sendo mais recomendado para uso;
- CCMP – *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*;
- WRAP – *Robust Authentication Protocol*.

Semelhante ao WPA, possui dois modos de operação, o Pessoal (baseado em PSK) e o Empresarial, que utiliza o 802.1x. No modo Pessoal, uma PSK deve ser configurada nos dispositivos. Ela pode conter até 64 caracteres ASCII. É possível também utilizar diretamente uma chave de 256bits gerados aleatoriamente, porém, essa abordagem dificulta o provisionamento dado que as

chaves tem que ser impostadas manualmente, tanto no AP quanto nos clientes (LASHKARI; DANESH; SAMADI, 2009).

### 3.5.1 *Wireless Robust Authenticated Protocol (WRAP)*

É o ultimo método de criptografia previsto no 802.11i. Assemelha-se ao CCMP. Usa AES para criptografia porém, em modo OCB. Este é um modo de operação para cifras de boco e foi projetado para prover integridade, autenticidade e confidencialidade. Ao contrário do CCMP que combina cifra de bloco em modo contador com CBC-MAC para realizar a mesma tarefa, sua intenção é trazer ganhos de performance. Entretanto, seu uso está restrito por patentes e portanto deve ser licenciado pelos fabricantes de dispositivos;.

### 3.5.2 *Counter Cipher Mode with CBC-MAC Protocol (CCMP)*

O *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol* ou apenas *Counter Cipher Mode Protocol*, é um método de criptografia que foi projetado para prover tanto confidencialidade como integridade e autenticidade das mensagens. Para confidencialidade faz uso do AES em modo contador. Para integridade e autenticidade utiliza o CBC-MAC, que funciona como uma espécie de assinatura eletrônica e consiste no último bloco de criptografia de uma mensagem cifrada usando alguma cifra de bloco em modo CBC. Neste caso, o próprio AES.

### 3.5.3 *Vulnerabilidades conhecidas do WPA2*

Com relação às vulnerabilidades, o WAP2 está sujeito aos mesmos problemas do WPA para redes em modo Pessoal utilizando senha (PSK). É importante atentar para o tamanho e complexidade das senhas utilizadas, buscando senhas maiores de 20 caracteres, a fim de mitigar ataques de dicionário e força bruta (LASHKARI; DANESH; SAMADI, 2009).

Com relação ao TKIP, este método de criptografia foi depreciado, portando não considera-se mais como vulnerabilidade do WPA2, embora, caso ainda esteja em uso, está sujeito aos mesmos problemas relatados nas seções anteriores.

### 3.6 Wi-fi Protected Setup (WPS)

Embora o WPS não seja um protocolo de 802.11, é importante falar sobre ele devido aos graves problemas de segurança que ele apresenta. Foi criado pela Wi-Fi Alliance e introduzido em 2006, com o principal objetivo de facilitar a configuração e habilitação do Wi-Fi *Protected Acces* e adição de novos dispositivos em ambientes domésticos, onde os usuários podem não ter os conhecimentos para realizar as configurações de segurança nos equipamentos, e consequentemente deixam suas redes desprotegidas.

Dispositivos que suportam o protocolo WPS são identificados pelos selos constantes na figura 5.

Figura 5 – Selos de identificação de dispositivos que suportam WPS


Fonte – Wi-Fi Alliance <http://www.wi-fi.org/about/wi-fi-brand>. Acessado em 28 de outubro de 2013.

O protocolo prevê quatro maneiras para adicionar novos dispositivos a rede:

- PIN (*Personal Identification Number*) – consiste em um código numérico de oito posições que deve ser lido da tela do aparelho a ser conectado na rede e impostado no AP por meio de uma interface de gerenciamento. Alternativamente pode ser realizado o processo inverso, com o PIN sendo lido da interface de gerenciamento e impostada no dispositivo. Esse método é obrigatório em dispositivos que suportam o protocolo;

- Botão – neste método o usuário simplesmente aperta um botão (que pode ser físico ou virtual) tanto no AP quanto no dispositivo a ser inserido na rede. A presença desse método é obrigatória em APs que suportam o protocolo e opcional nos demais dispositivos;
- NFC (*Near-Field-Communication*) – nessa modalidade o usuário simplesmente aproxima um dispositivo que possua NFC habilitado do AP. O suporte deste método é opcional;
- USB – neste método o usuário utiliza um *pendrive* entre o dispositivo cliente e o AP. Também é opcional.

### 3.6.1 *Vulnerabilidades conhecidas do WPS*

Os maiores problemas existentes no WPS estão relacionados implementações ruins do protocolo, principalmente quanto ao uso do PIN para adição de novos dispositivos. As principais falhas estão relacionadas a não implementação de mecanismo que tratem múltiplas ocorrências de pins digitados errados em sequência. Isso possibilita ataques de força bruta no WPS que são muitas vezes mais rápidos do que a quebra das PSK.

Existem ferramentas disponíveis (a exemplo do reaver) que exploram essa vulnerabilidade para conseguir acesso a redes independentemente qualidade das configurações do WPA2.

# 4 SEGURANÇA DAS REDES NO PLANO PILOTO

Os capítulos anteriores deste trabalho tratam do funcionamento das redes sem fio. Por meio de pesquisa bibliográfica são apresentadas análises dos algoritmos e protocolos de segurança aplicados no padrão 802.11 dando ênfase nas vulnerabilidades e problemas reportados até o momento. São explorados também riscos associados ao uso desta tecnologia, a cada dia mais presente e mais ubíqua. Sem dúvida uma ferramenta essencial em um universo dominado por dispositivos móveis.

Conforme viu-se, muitos dos mecanismos de segurança propostos para essas redes ficaram rapidamente defasados, não sendo mais capazes de exercerem seu papel de forma eficaz. O que levou a necessidade de aperfeiçoamento e desenvolvimento de novos mecanismos de proteção. A velocidade com que estas mudanças ocorreram criou um cenário de convivência entre dispositivos novos e antigos, que não suportam as novas tecnologias de proteção. Em consequência disso, concentradores de redes sem fio (AP's) necessitam de suportar diversos protocolos de segurança, mesmo que estes não sejam os mais novos ou mais seguros.

Cabe ao administrador da rede determinar quais mecanismos de segurança serão adotados e permitidos. Ambientes em que existem equipamentos mais antigos podem necessitar de usar protocolos de segurança defasados. Essa decisão leva em consideração diversos fatores como as capacidades dos dispositivos, disponibilidade de orçamento para atualização de equipamentos e principalmente, uma análise de risco que identifique as ameaças e consequências de eventos adversos, decorrentes da exploração de vulnerabilidades da rede.

É claro que muitas redes também podem apresentar problemas de segurança decorrentes de uma gestão ruim, desconhecimentos dos problemas existentes e falta de capacidade técnica para sua correção. O que geralmente é reflexo da ausência de análise de risco apropriada. É possível supor que a ocorrência desses problemas sejam mais frequentes em cenários de uso doméstico e em pequenas empresas, dado que sua disponibilidade de recursos tende a ser menor.

O presente trabalho propõe um estudo das redes sem fio localizadas na região central da capital federal, conhecida como Plano Piloto, para observar aspectos de segurança, tomando como base determinados parâmetros das redes que podem ser coletados de forma passiva, conforme descrito a seguir.

## 4.1 Metodologia

Para o cumprimento dos objetivos propostos por este trabalho optou-se por utilizar a técnica conhecida como *Wardrive,* que consiste em utilizar um veículo para percorrer um trajeto e ao mesmo tempo utilizar equipamentos (*hardware e software*) que possibilitem monitorar a atividade das redes presentes no caminho. Desse modo foi possível coletar uma amostra para realização da análise.

Adotou-se uma estratégia para permitir a comparação entre diferentes cenários de utilização que tira proveito do fato de Brasília ser uma cidade planejada. A região conhecida como Plano Piloto é totalmente setorizada, dividida em áreas que visam facilitar a concentração de empresas de um mesmo segmento. Essa característica permitiu a separação dos dados coletados de acordo com as destinações das áreas geográficas, permitindo agrupar dados de áreas com destinações semelhantes e comparar com dados de áreas com destinações diferentes.

Para o planejamento e execução realizou-se os seguintes passos:

- Testes com equipamentos e softwares necessários para captura dos dados, afim de determinar a melhor configuração;
- Identificação de parâmetros disponíveis para análise;
- Escolha das regiões geográficas da cidade em que seriam realizadas as coletas de dados;
- Demarcação de um perímetro para cada região;
- Determinação uma rota para a realização da captura dos dados;
- Coleta dos dados;
- Por fim, o processamento e análise dos dados.

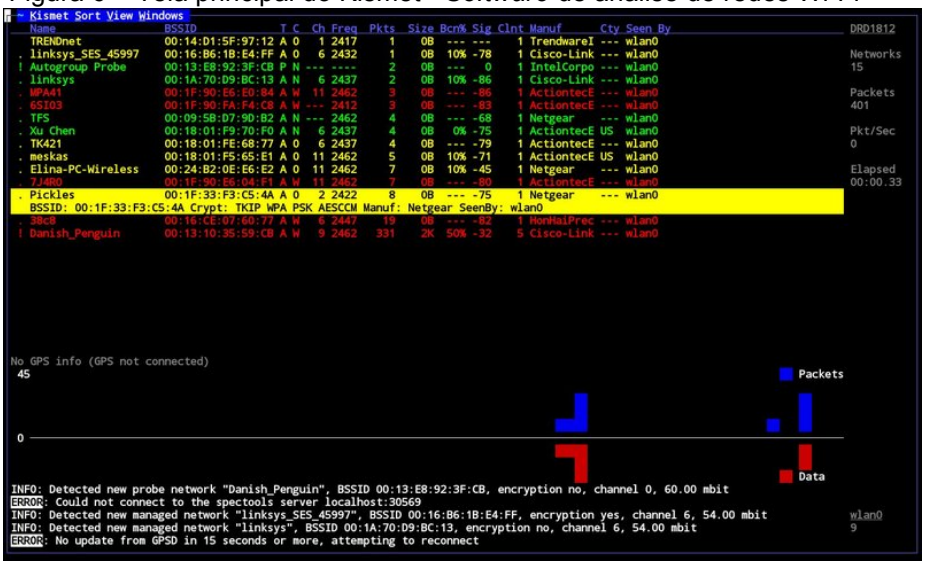
### 4.1.1 *Software e equipamentos*

Para possibilitar a coleta de dados, utilizou-se e equipamentos de uso geral, ou seja, que não foram desenvolvidos especificamente para realização deste tipo de atividade. Estes equipamentos podem ser encontrados em lojas de informática e são destinados principalmente a uso doméstico.

O ponto chave da coleta de dados é o uso de um conjunto de *softwares* especificamente desenvolvidos para auditoria, análise e monitoramento de redes sem fio. Esse conjunto é composto por *softwares* de baixo nível, que interagem diretamente com os equipamentos físicos e são capazes de faze-los funcionar de um modo não convencional, possibilitando a monitoração das redes sem fio. Também é necessário o programa que atua no nível mais alto, tratando os dados coletados pelos equipamentos e disponibilizando interface para o usuário.

O programa escolhido para esse propósito foi o Kismet. Um *software* de código aberto que é considerado um dos mais completos para o proposito que se quer. Apesar de sua interface gráfica ser baseada em caracteres, é uma ferramenta muito poderosa e que permite a extração de dados em diversos formatos, o que facilita a utilização de outras ferramentas para análise. A figura 6 apresenta a tela do programa. Uma característica importante do Kismet é que ele permite a associação das redes com sua localização geográfica fazendo uso de dados providos por um equipamento de GPS.

Figura 6 – Tela principal do Kismet - *Software* de análise de redes Wi-Fi

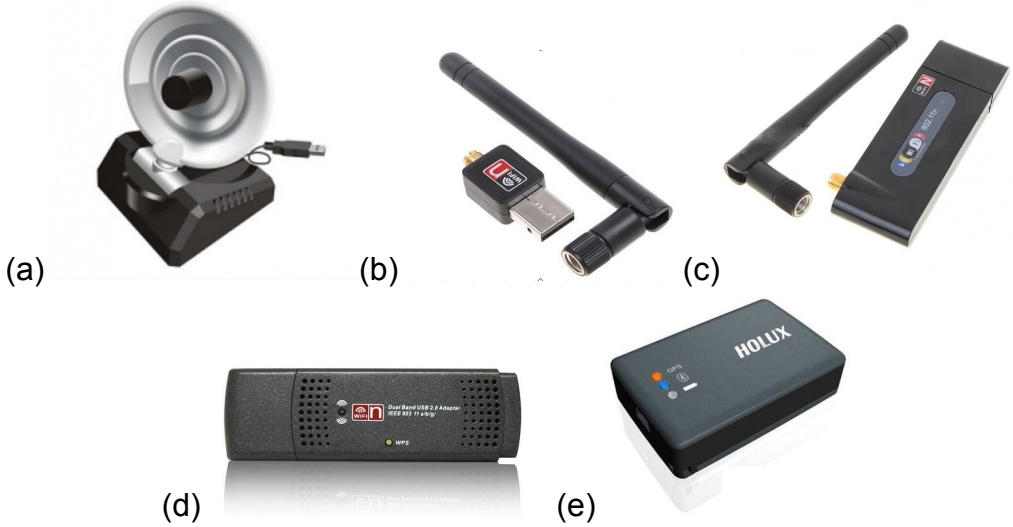



Fonte – Capturado da tela do sistema com o programa em execução.

Com relação aos equipamentos de *hardware* foi utilizado um computador portátil (*notebook*) com sistema operacional Ubuntu Linux. Foram conectados ao computador quatro placas de redes sem fio por meio da interface USB, sendo que três delas possuíam antenas externas. Uma delas direcional (figura 7, a) e as outras duas omnidirecionais (figura 7, “b“ e “c”), que possibilitam a captura de sinais de qualquer direção. Todas as antenas são compatíveis com os padrões 802.11b/g/n. A antena da figura 7 “d” trabalha tanto na frequência de 2,4GHz quanto em 5GHz, o que permitiu a coleta de dados de redes no padrão 802.11a.

Foi utilizado também um equipamento de GPS (*Global Positioning System*), representado na figura 7 “e”. Este equipamento utiliza-se de sinais emitidos por satélites para determinar sua posição no globo terrestre. O modelo de equipamento utilizado, permite que as informações de localização obtidas sejam transmitidas para outros dispositivos por meio de interface *bluetooth* (sem fio) e também USB.

Figura 7 – Equipamentos utilizados




(a) (b) (c)

(d) (e)

Fonte –

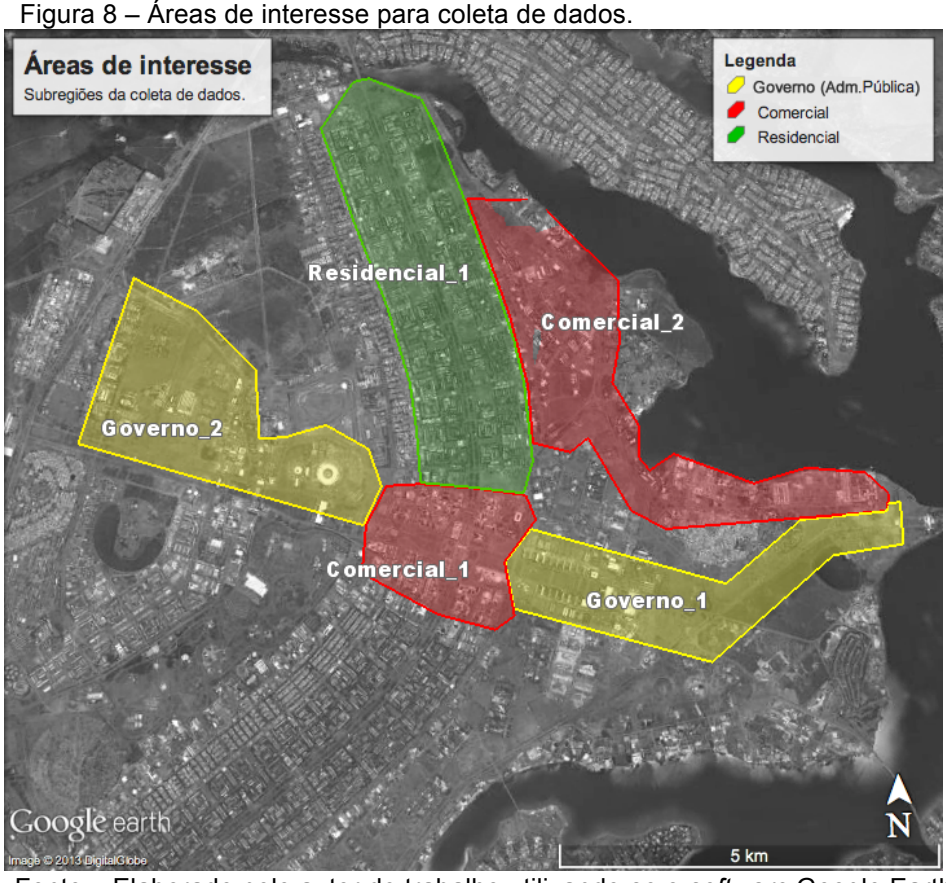
As especificações técnicas dos equipamentos podem ser consultadas no anexo A.

### 4.1.2 *Delimitação de regiões de coleta de dados*

O foco da observação está na região do Plano Piloto, em Brasília no Distrito Federal. Essa localidade tem a característica interessante de ser totalmente setorizada, dividida em áreas que visam facilitar a concentração de empresas de um mesmo segmento, tais como: Setor Bancário, Setor Comercial, Setor Hospitalar, Setor de Diversões, Setor de Autarquias, Setor de Clubes, Setor de Embaixadas, áreas residenciais, comerciais locais, dentre outras.

Assim, adotou-se a estratégia de demarcar algumas áreas que representassem o Plano Piloto como um todo. Essas áreas ou regiões (5 ao todo) são compostas por um ou mais setores determinados no planejamento urbano da cidade e foram demarcadas de modo a conter setores com características de destinação semelhante. Cada uma delas foi classificada dentro de um dos três grupos: Governo, Comercial e Residencial. O perímetro das 5 regiões demarcadas ficou conforme ilustrado na figura 8.

Figura 8 – Áreas de interesse para coleta de dados.




Fonte – Elaborado pelo autor do trabalho utilizando-se o *software* Google Earth.

O grupo Governo é composto por áreas que tem a característica de serem ocupadas principalmente por edifício de órgão da administração pública entidades relacionadas ao governo. O grupo Comercial tem foco em empresas de médio e grande porte e o grupo Residencial é composto por áreas residenciais. Seu detalhamento consta no quadro 3.

Quadro 3 – Detalhamentos dos Grupos e Regiões de coleta de dados.

| Grupo | Região | Características | Descrição da composição |
|---|---|---|---|
| **Governo** | Governo_1 | Perímetro: 13,4Km<br>Área: 4,91Km$^2$ | Área ocupada por entidade do Governo Federal. Esplanada dos ministérios e áreas de residências oficiais. Prédios mais baixos (até 10 andares) e com mais áreas abertas. |
| | Governo_2 | Perímetro: 12,4Km<br>Área: 6,46Km$^2$ | Setor militar e áreas de entidades do Governo do Distrito Federal. Possui muitos espaços abertos e prédios baixos (até 6 andares). |
| **Comercial** | Comercial_1 | Perímetro: 7,26Km<br>Área: 3,34Km$^2$ | Composta pelos setores: Comercial; de Diversões; Hoteleiro; de Autarquias; Bancário. Área ocupada por prédio altos para o padrão de Brasília (até 25 andares) e muito próximos fisicamente. |
| | Comercial_2 | Perímetro: 18,7Km<br>Área: 7,83Km$^2$ | Área ocupada em grande parte por universidades, escolas e hotéis. Abriga também o Setor de Clubes Norte. Muitas áreas abertas e prédios baixos (até 6 andares). |
| **Residencial** | Residencial | Perímetro: 14,8Km<br>Área: 9,50Km$^2$ | Área composta apenas por prédios com até 6 andares. Contempla as chamadas Super Quadras Norte (destinação residencial) e as Comerciais Locais Norte que consistem em pequenas edificações comerciais (até 3 andares) destinadas a mercados, padarias, lojas, restaurantes e bares (ocorrem a cada intervalo de 2 super quadras). |

Fonte – Elaborado pelo autor do trabalho.

É importante salientar que a classificação das regiões em grupos não é absoluta, ou seja, pode haver redes encontradas em uma região que sejam utilizadas para propósitos que se encaixem melhor em outro grupo. Por exemplo, na região classificada como residencial existem diversas áreas de comércio, os chamados comércios locais, entretanto a maioria dos edifícios é de destinação exclusivamente residencial. Dificilmente haverá uma grande empresa situada nesta área. Já no caso das regiões marcadas como comerciais, não pode-se assumir que não existam pessoas morando nestas áreas, e que portanto não haverá redes de

uso doméstico. As regiões foram classificadas de acordo com sua principal destinação para permitir a observação de possíveis peculiaridades de cada público.

As coordenadas geográficas das regiões demarcadas podem ser encontradas no apêndice A.

### 4.1.3 *Trajeto percorrido*

O trajeto percorrido para coleta dos dados durante o *wardrive* está representado pela linha vermelha desenhada no mapa da figura 9. A distância total percorrida foi de 68,1Km, a uma velocidade média de 26,47Km/h (desconsiderado o tempo em que o veículo ficou parado). A atividade foi iniciada no dia 19 de outubro de 2013 às 23h30 e teve duração aproximada de 2 horas e 30 minutos.

Figura 9 – Trajeto percorrido na realização do *Wardrive*.


Fonte – Elaborado pelo autor do trabalho, utilizando-se o aplicativo Trails Lite para iPad.

## 4.2 Análise de dados

O *software* Kismet coleta diversos dados. Selecionou-se apenas alguns considerados interessantes para as análises. São eles:

- Modo da rede (infraestrutura ou Ad-Hoc);
- ESSID (nome da rede);

- Fabricante do equipamento:  (derivado a partir do BSSID da rede);
- Canal de comunicação utilizado;
- Rede oculta (se realiza broadcast do ESSID);
- Criptografia;
- Manor localização (latitude e longitude);
- Maior localização (latitude e longitude);
- Melhor localização (latitude e longitude onde o sinal foi mais forte).

### 4.2.1 *Resumo dos dados coletados*

Na coleta de dados foram identificados 12.859 concentradores de rede. O que representa uma média de 188 redes a cada quilometro percorrido, ou uma rede a cada 5,3 metros aproximadamente. Um contraste grande com a densidade de redes encontradas na região Comercial_1, onde foram percorridos aproximadamente 8Km e localizadas 4.538 redes, com média de aproximada de 533 redes por quilômetro ou uma rede a cada 1,9 metros. Uma densidade correspondente a 2,8 vezes a densidade média. O quadro 4 resume a quantidade de redes coletadas por região.

Quadro 4 – Redes por grupo e região.

| Grupo | Região | Qtd. de APs | TOTAL |
|---|---|---|---|
| **Comercial** | Comercial_1 | 4.538 | 6.032 |
| | Comercial_2 | 1.494 | |
| **Governo** | Governo_1 | 1.601 | 1.990 |
| | Governo_2 | 389 | |
| **Residencial** | Residencial_1 | 4.837 | 4.837 |
| **TOTAL** | | | **12.859** |

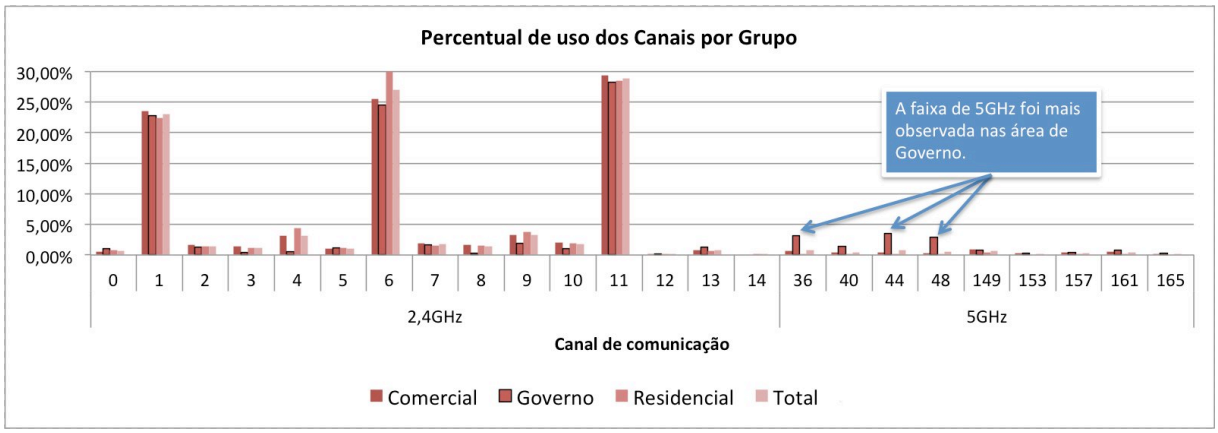
Fonte – Elaborado pelo autor do trabalho.

### 4.2.2 *Descrição de achados*

Com relação a distribuição de uso dos canais de comunicação do 802.11, foi possível observar que os canais 1, 6 e 11, que são os canais de operação padrão configurados de fábrica, estão saturados. Mais de 90% das redes observadas utiliza um dos 3 canais, e sua distribuição é quase uniforme em qualquer dos grupos observados. Em áreas onde há grande densidade de redes como na região Comercial_1, conforme pode ser observado no quadro 4, pode haver grande interferência de uma rede na outra. Na figura, o tamanho dos círculos que representam a rede correspondem a uma estimativa de sua potência baseada no tamanho da área onde foi possível capturar o sinal. Vê-se que dificilmente um circulo não intersecta outro.

Observa-se que os demais canais estão mal aproveitados. Nesses casos uma análise de espectro poderia ajudar a determinar o canal com menor interferência para uma determina rede, trazendo possíveis ganhos de desempenho e melhorando a disponibilidade do serviço.

Gráfico 1 – Percentual de uso dos canais de comunicação por grupo.

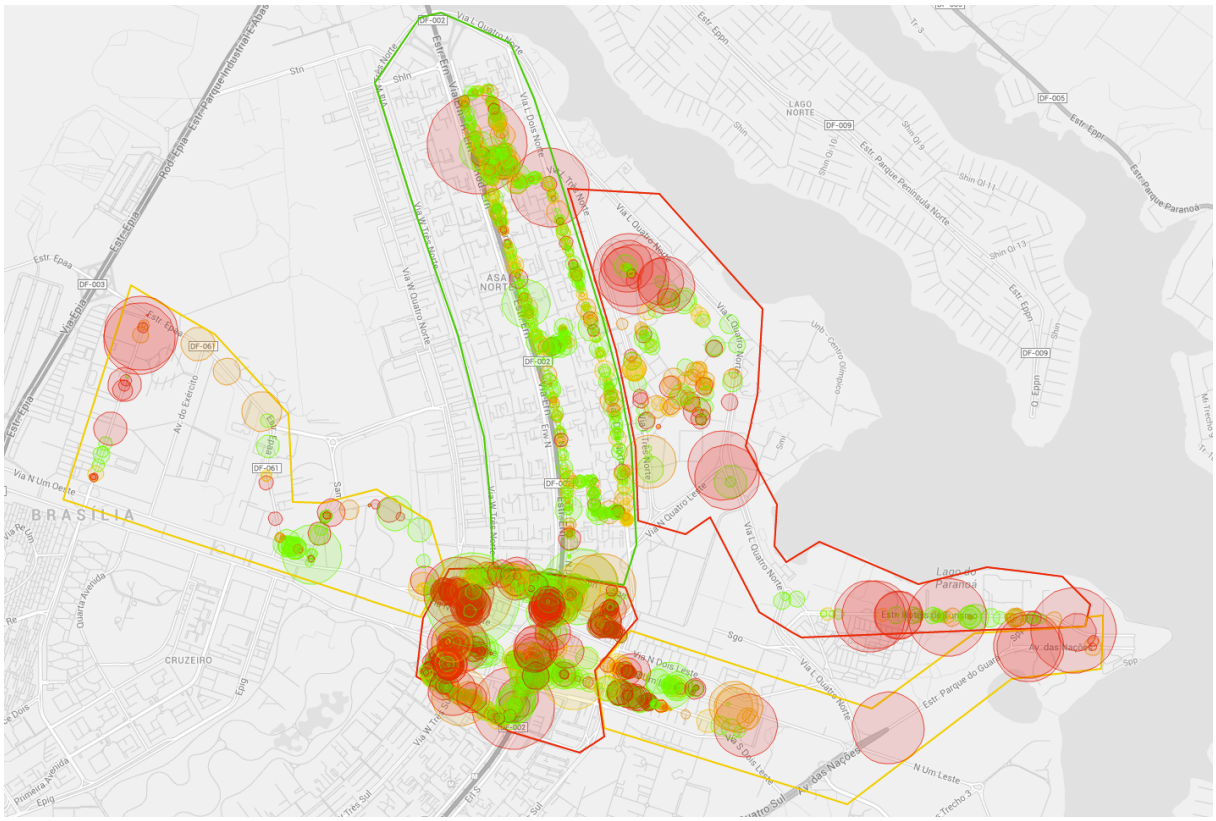



Fonte – Elaborado pelo autor do trabalho.

É possível observar que a grande maioria das redes (95,56%) estão operando na frequência de 2,4GHz, do que se pode inferir que operam no padrão b, g ou n. Outro ponto interessante é o fato de que a grande maioria das redes operando em 5GHz (possivelmente padrão a) pertence ao grupo Governo.

A figura 10 representa 20% da amostra de dados coletados. Foi adotada uma escala de cores do verde ao vermelho, em relação à implementação dos protocolos de segurança. Em que verde representa as redes com protocolos mais seguros e vermelho representa as redes abertas.

Figura 10 – Amostra aleatória de 20% das redes sem fio coletadas.




Fonte – Elaborado pelo autor do trabalho. Cada círculo representa uma rede. O tamanho do círculo é uma estimativa de potência calculada com base na distância entre o ponto máximo e mínimo onde a rede foi observada. Redes verdes possuem o protocolo WPA-AES-CCMP, amarelas estão utilizando WPA-TKIP, laranjas WEP e vermelhas estão sem criptografia.

Com relação aos fabricantes dos equipamentos, este dado foi inferido com base em seu BSSID, pois este código deve único para cada equipamento, de modo que cada fabricante tem uma faixa numérica de numeração. Os resultados obtidos estão representados no gráfico 2, sendo que observou-se que 70% dos equipamentos foram fornecidos por 19 fabricantes. Outros 12% foram fornecidos por 102 fabricantes e não foi possível identificar o fabricante de 18% deles.

Não foi feita relação desse dado com as características de segurança das redes, de modo que o dado serve a propósitos meramente informativos.

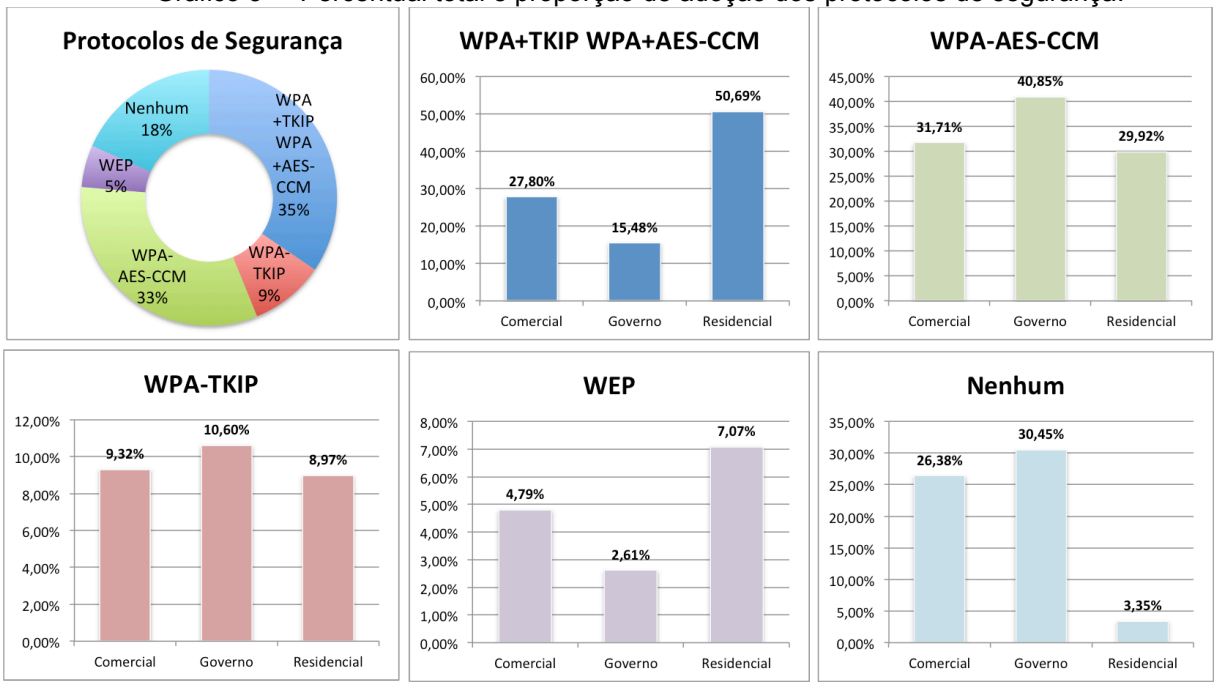
Gráfico 2 – Percentual de equipamentos por fabricante.


Fonte – Elaborado pelo autor do trabalho.

Com relação aos protocolos de segurança (gráfico 3) observou-se que 82% das redes estão protegidas por algum dos recursos de segurança do 802.11. 68% suportam o WPA2 (designado pelo WPA-AES-CCM) embora 35% destes ainda mantenham retro compatibilidade com o WPA (WPA-TKIP), sendo observada a maior proporção de dispositivos com retro compatibilidade no grupo Residencial.

O uso exclusivamente do WPA foi observado em 9% dos equipamentos, sendo a proporção um pouco maior no grupo Governo. A presença do WEP ainda é observada, apesar de toda publicidade negativa que sofreu nos últimos anos. **5% dos equipamentos observados ainda utilizam WEP**, sendo a **menor** incidência no grupo Governo. É importante lembrar que ferramentas disponíveis livremente quebram, hoje, o WEP em questão de minutos.

Gráfico 3 – Percentual total e proporção de adoção dos protocolos de segurança.



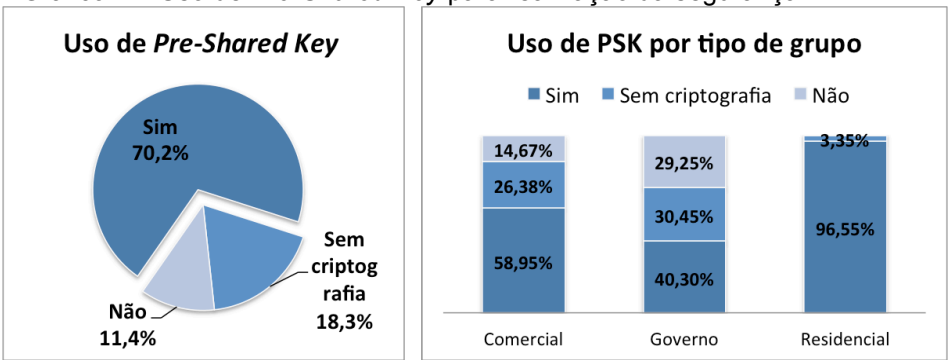

Fonte – Elaborado pelo autor do trabalho, onde “WPA-AES-CCM” corresponde ao WPA2; “WPA-TKIP” corresponde ao WPA e “WPA-TKIP WPA-AES-CCM” ao WPA2 com compatibilidade.

É possível observar que 18% das redes foram marcadas como abertas. A princípio sem nenhuma segurança. É o caso de redes de acesso público em que o usuário se conecta a rede e em seguida é autenticado por meio de um recurso conhecido como "*Captive Portal*". Nesse caso todo o tráfego do usuário é bloqueado até que ele abra um navegador de internet, onde será redirecionado para uma página de autenticação. Nestes casos, mesmo o acesso a rede dependa de autenticação existem vulnerabilidades que podem ser exploradas para se ganhar acesso não autorizado a rede. Além disso, o tráfego entre AP e cliente é transmitido em claro.

Redes que utilizam 802.1x também aparecerão como abertas. Como possivelmente é o caso de parte ou o todo dos 30% das redes do grupo Governo marcadas como abertas e parte do grupo Comercial. O que não significa de modo algum que estas redes estejam desprotegidas. O 802.1x possui estratégias diferentes para proteger a comunicação que não ficam explícitas pelo método de coleta de dados. É importante ressaltar que apenas 3,35% das redes do grupo Residencial encontram-se abertas e provavelmente totalmente desprotegidas. É um percentual relativamente baixo, entretanto o objetivo deve ser de que todas as redes estejam protegidas.

Como pode ser observado no gráfico 4, 70% das redes protegidas utilizam *Pre-Shared Key* (senha compartilhada) para autenticação. Disso pode-se concluir que muitas destas redes estão vulneráveis e portanto susceptíveis a ataques.

Gráfico 4 – Uso de *Pre-Shared Key* para realização da segurança.




Fonte – Elaborado pelo autor do trabalho.

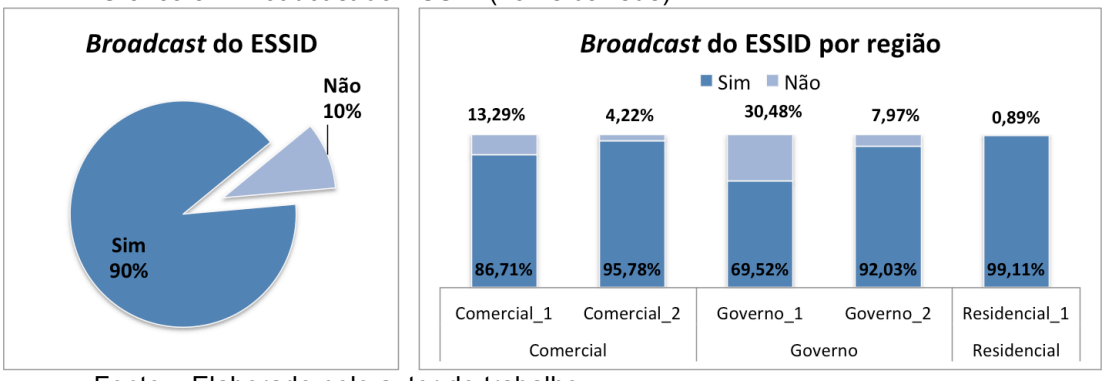
Nos capítulos anteriores viu-se que existem mecanismos como o ataque de dicionário, ou mesmo o de força bruta, capazes de que quebrar as senhas

utilizadas pelas redes. Nesse percentual inclui-se ainda as redes WEP, extremamente fáceis de serem atacadas. É importante ainda lembrar que existem serviços pagos para quebra das senhas destas redes, a exemplo do cloudcracker.com que cobra 17 dólares por senha quebrada. Conforme visto anteriormente, a única forma de proteção contra estes ataques é o uso de senhas longas e com caracteres diversificados (mais de 20 caracteres, contendo letras, números e caracteres especiais como sinais de pontuação e caracteres acentuados).

É interessante observar também que 96,5% das redes do grupo Residencial utilizam essa estratégia para proteção, que trás problemas para o gerenciamento da rede. Dado que o gerenciamento das senhas é manual, em um ambiente com poucos usuários é mais fácil distribuir uma nova senha. Mesmo assim, é sabido que as pessoas tendem a manter a mesma senha por uma questão de comodidade. Quando se fala de um ambiente corporativo, com muitos usuários, fica impossível gerencia a rede desta maneira.

Uma estratégia de segurança complementar é desabilitar o mecanismo de *broadcast* da presença da rede. Isso faz com que os usuários necessitem de saber previamente da existência da rede, bem como dos parâmetros necessários ao acesso, incluso ai o próprio nome da rede. Observou-se que 10% das redes utiliza-se desta estratégia (gráfico 5), sendo seu uso mais frequente na região Governo_1 em 30% das redes.

Gráfico 5 – *Broadcast* do ESSID (nome da rede).




Fonte – Elaborado pelo autor do trabalho.

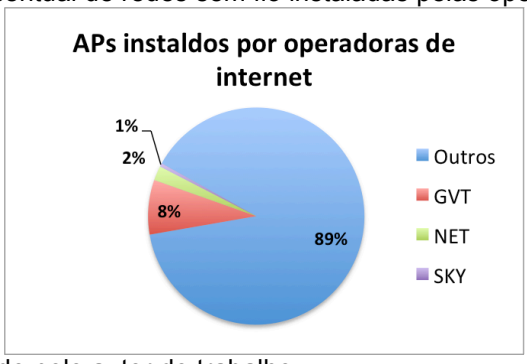
Outro aspecto interessante observado diz respeito às redes sem fio instaladas por empresas prestadoras de serviço de internet. Muitas delas estão

oferecendo a instalação de redes sem fio juntamente com o serviço de internet como um diferencial de mercado.

Filtrou-se por meio do ESSID das redes os equipamentos instalados por três das operadoras que prestam esse serviço. A GVT possui um padrão facilmente identificável para o nome de suas redes que é composto pelo nome “GVT-“ e um código hexadecimal de 4 posições. No caso da NET utilizou-se a busca pela palavra chave “virtua“ que faz alusão ao seu serviço NET Virtua. A provedora SKY também adota um padrão bem definido para suas redes. Ele consistem na palavra “SKY_” associada a um código hexadecimal de seis posições.

Com relação as redes fornecidas observou-se que correspondem a 10,8% do total das redes sem fio, sendo 74% delas no grupo Residencial, 24% no Comercial e apenas 1% no Governo. Constatou-se também que desses 10,8%, 75% foram instaladas pela GVT, 20% pela NET e 5% pela SKY. A proporção em relação ao total de redes é apresentada no gráfico 6.

Gráfico 6 – Percentual de redes sem fio instaladas pelas operadoras GVT, NET e SKY.



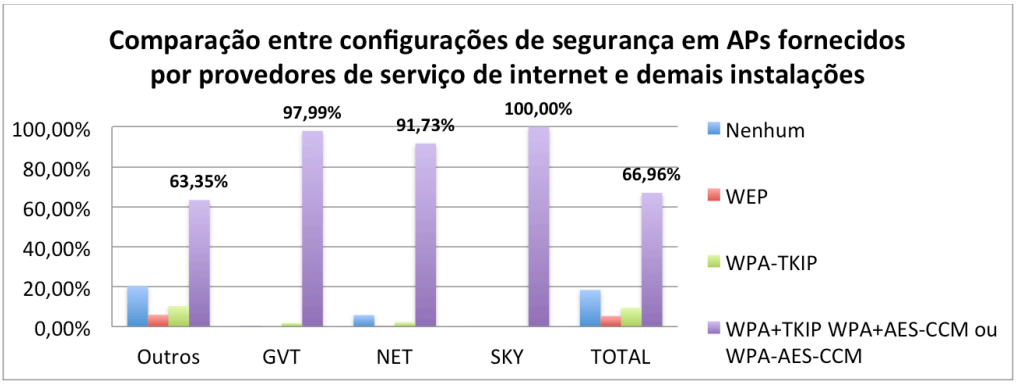

Fonte – Elaborado pelo autor do trabalho.

O porque do percentual das redes instaladas pelas operadoras ser um fato interessante é evidenciado pelo gráfico 7 que compara a criptografia adotada nessas redes com as demais redes encontradas e também com o total delas. A média proporcional de adoção do WPA2 é nestas redes é maior do que 90% em qualquer operadora. A media geral para as redes por operadoras ultrapassa os 99%. Destaque para a SKY, em que 100% das redes utiliza o WPA2.

Esses valores contrastam com as proporções das demais redes (63,3%), do total (66,9%) observados no gráfico 7 e também da proporção geral das redes do grupo Residencial que é de 80,6%. Estes dados evidenciam que as operadoras estão contribuindo para o aumento dos padrões de segurança das redes sem fio ao

trazerem para si a responsabilidade pela instalação da rede e em consequência pela segurança.

Gráfico 7 – .




Fonte – Elaborado pelo autor do trabalho.

É importante observar também que a diversificação dos nomes das redes (ESSID) é importante para dificultar ataques de força bruta para quebra da PSK da rede. Viu-se que a utilização de nomes de redes padronizados favorece a utilização de *rainbow tables* para acelerar o processo de quebra das chaves. Observa-se a implementação dessa boa prática pela GVT e SKY ao utilizarem um código pseudoaleatório para compor o nome das redes em seus equipamentos.

# CONCLUSÃO

A partir deste estudo foi possível compreender melhor os riscos e problemas associados ao uso de redes Wi-Fi. Foi possível também, identificar a forma com que os protocolos de segurança presentes no padrão IEEE 802.11 atuam na mitigação destes riscos, onde obtêm êxito e também seus pontos de falha. A partir destes conhecimentos buscou-se uma abordagem prática que permitisse traçar um paralelo entre os problemas identificados nas tecnologias e sua incidência em um contexto real (Plano Piloto, Brasília). Foi possível identificar regiões da cidade em que existiu a predominância de determinados mecanismos de proteção. Com base nos setores bem demarcados do Plano Piloto, estabeleceu-se um paralelo entre três perfis determinados de usuários e sua adoção/preferencia por determinados métodos de proteção. Identificou-se também áreas de maior concentração de redes.

Observou-se a existência de espaço para melhoria da segurança das redes sem fio. Viu-se também que o uso de senhas compartilhadas (PSK) é um mecanismo muito popular para proteção de redes sem fio. Ele faz muito sentido em ambientes domésticos e de pequenas empresas, entretanto sua presença é expressiva em determinadas regiões da cidade ocupadas predominantemente por entidades vinculadas ao governo, grandes e médias empresas. Identificou-se que empresas de telecom. vêm oferecendo a seus clientes, a instalação de redes sem fio em conjunto com o serviço de internet. Fato que as torna agentes importantes para a melhoria da segurança das redes sem fio da cidade, na medida em que assumem a responsabilidade pela instalação dessas redes e em consequência pelas configurações de segurança. Observou-se que seu trabalho vem contribuindo de forma efetiva para o alcance desse objetivo.

Em resumo, foi possível identificar boas práticas de segurança em aplicação, iniciativas que estão impactando positivamente na segurança, bem como identificar pontos de melhoria. Apesar de tudo, é importante lembrar que a segurança nunca deve se basear em apenas uma medida ou camada de proteção.

# REFERÊNCIAS


ALFARDAN, N. et al. On the Security of RC4 in TLS and WPA. In: USENIX SECURITY SYMPOSIUM, 22, 2013, Washington. 2013. Disponível em: <http://profs.info.uaic.ro/~fltiplea/CC/ABPPS2013.pdf >. Acesso em: 26 out. 2013.

BORISOV, N.; GOLDBERG, I.; WAGNER, D. Intercepting mobile communications: the insecurity of 802.11. In: MobiCom, 01, 2001, Roma. **Proceedings...** New York: ACM, 2001. p. 180-189.

BRASIL. Câmara dos Deputados. **PL 2126/2011**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL+2126/2011>. Acesso em: 26 out. 2013.

FAROOQ, T; JONES, D. L.; MERABTI, M. MAC Layer DoS Attacks in IEEE 802.11 Networks. In: THE 11TH ANNUAL CONFERENCE ON THE CONVERGENCE OF TELECOMMUNICATIONS, NETWORKING AND BROADCASTING (PGNET). 2010.

GOLD, Steve. Cracking wireless networks. **Network Security**, v. 2011, n. 11, p. 14-18, 2011.

GUENNOUN, M. et al. Wireless networks security: Proof of chopchop attack. In: INTERNATIONAL SYMPOSIUM ON A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS (WoWMoM), 2008, Newport Beach. **Anais eletrônicos...** IEEE, 2008. p. 1-4. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4594924>. Acesso em: 21 out. 2013.

GURKAS, G. Z.; ZAIM, A.H.; AYDIN, M. A. Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks. In: INTERNATIONAL SYMPOSIUM ON COMPUTER NETWORKS, 2006, Istanbul. **Anais eletrônicos...** IEEE, 2006. p. 1-5. Disponível em: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1662520>. Acesso em: 12 out. 2013.

HOWLETT, T. **Open source security tools**: practical applications for security. New Jersey: Pearson Prentice Hall, 2005.

HUANG, J. et al. Security Analysis of Michael: The IEEE 802.11 i Message Integrity Code. **Embedded and Ubiquitous Computing – EUC**, Heidelberg, v. 3823, 2005. Berlin: Springer, 2005. p. 423-432. Disponível em: <http://link.springer.com/chapter/10.1007/11596042_44>. Acesso em: 2 out. 2013.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. IEEE Standard for Information technology. Telecommunications and information exchange between systems Local and metropolitan area networks. **Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Ame.** 2012.
Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=STDPD97235>. Acesso em: 17 out. 2013.

ISO, ABNT NBR. IEC 27001: 2006: Tecnologia da Informação–Técnicas de segurança–Sistemas de gestão de segurança da informação-Requisitos.**Associação Brasileira de Normas Técnicas**, 2006.

KUROSE, J. F; ROSS, K. W. **Redes de computadores e a internet:** Uma abordagem top-down. 3. ed. São Paulo: Pearson Addison Wesley, 2006.

LASHKARI, A. H.; DANESH, M. M. S.; SAMADI, B. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In: IEEE INTERNATIONAL CONFERENCE ON COMPUTER SCIENCE AND INFORMATION TECHNOLOGY (ICCSIT), 02, 2009, Beijing. **Anais eletrônicos...** IEEE, 2009. p. 48-52. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5234856>. Acesso em: 26 out. 2013.

MENEZES, A. J; OORSCHOT, P. C; VANSTONE, S. A. **Handbook of applied cryptography**. CRC Press, 2001.

MOEN, V.; RADDUM, H.; HOLE, K. J. Weaknesses in the Temporal Key Hash of WPA. **ACM SIGMOBILE Mobile Computing and Communication Rev**. New York:ACM, v. 8, n. 2, 2004. p. 76-83. Disponível em: <http://dl.acm.org/citation.cfm?id=997132>. Acesso em: 17 out. 2013.

NASR, K.; EL KALAM, A. A.; FRABOUL, C. A holistic methodology for evaluating wireless Intrusion Detection Systems. In: INTERNATIONAL CONFERENCE ON NETWORK AND SYSTEM SECURITY (NSS), 5, 2011, Milão. **Anais eletrônicos...** IEEE, 2011. p. 9-16. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6059954>. Acesso em: 21 out. 2013.

NISBET, A. A Tale of Four Cities: Wireless Security & Growth in New Zealand. In: INTERNATIONAL CONFERENCE ON COMPUTING, NETWORKING AND COMMUNICATIONS (ICNC), 2012, Maui. **Anais eletrônicos...** IEEE, 2012. p. 1167-1171. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6167391>. Acesso em: 21 out. 2013.

PATTERSON, D. A; HENNESSY, J. L. **Organização e projeto de computadores:** A interface hardware/software. 3. ed. Rio de Janeiro: Elsevier, 2005.

PEISONG, Y; GUANGXUE, Y. Security Research on WEP of WLAN. In: INTERNATIONAL SYMPOSIUM ON NETWORKING AND NETWORK SECURITY, 10, Jinggangshan, 2010. **Proceedings...** Jinggangshan, 2010. p. 39–42.

RUFINO, N. M. O. **Segurança em redes sem fio:** Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth. 3. ed. São Paulo: Novatec Editora, 2011.

SIVAKUMAR, C.; VELMURUGAN, A. High Speed VLSI Design CCMP AES Cipher for WLAN (IEEE 802.11 I). In: INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING, COMMUNICATIONS AND NETWORKING (ICSCN), 07, 2007, Chennai. **Anais eletrônicos...** IEEE, 2007. p. 398-403. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4156652>. Acesso em: 21 out. 2013.

SRIVATSA, M. Who is Listening? Security in Wireless Networks. In: INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING, COMMUNICATIONS AND NETWORKING (ICSCN), 08, 2008, Chennai. **Anais eletrônicos...** IEEE, 2008. p.167-172. Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4447182>. Acesso em: 21 out. 2013.

TANENBAUM, A. S; WETHERALL, D. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

VIEHBÖCK, S. Brute Forcing Wi-Fi Protected Setup. 2011. Disponível em: <http://www.coyotus.com/repo/pdf/hacking/viehboeck_wps.pdf>. Acesso em: 26 out. 2013.

WALKER, J. el al. Unsafe at any key size; an analysis of the WEP encapsulation. IEEE document. v. 802, pp. 362, 2000.

WONG, S. The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. v. 28, n. 7, p. 05, 2003. Disponível em: <http://www.sans.org/reading-room/whitepapers/wireless/evolution-wireless-security-80211-networks-wep-wpa-80211-standards-1109> Acesso em: 17 out. 2013.

ZHAO, S; SHONIREGUN, C. Critical Review of Unsecured WEP. In: IEEE CONGRESS ON SERVICES, 2007, Salt Lake City. **Anais eletrônicos...** IEEE, 2007. p. 368–374. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4278820>. Acesso em: 26 out. 2013.

## APÊNDICE A – Demarcações geográficas das regiões

Os perímetros de cada um das regiões geográficas determinadas são demarcados pelos polígonos formados pela união dos pontos marcados pelas coordenadas a seguir:

- **Governo**
  - Governo_1

    (-15.8010329846136,-47.8762777092128),
    (-15.8084005028605,-47.8516746829297),
    (-15.7962350249813,-47.8350068649475),
    (-15.7952563489608,-47.8258777992559),
    (-15.7915649578681,-47.8257462759151),
    (-15.7900195969152,-47.8257240176132),
    (-15.7902094830032,-47.8273318480397),
    (-15.7911339734258,-47.8275535122060),
    (-15.7917369712951,-47.8388000006120),
    (-15.7991211191548,-47.8491391552350),
    (-15.7914816163127,-47.8736339474590),
    (-15.7953831760601,-47.8771466236230),
    (-15.8010329846136,-47.8762777092128);

  - Governo_2

    (-15.7855587432453,-47.8924876080930),
    (-15.7808949590415,-47.8939764795608),
    (-15.7776927245792,-47.8993470839521),
    (-15.7790361974695,-47.9047039149788),
    (-15.7789940507097,-47.9078749575853),
    (-15.7703873229271,-47.9083182087262),
    (-15.7625722481331,-47.9157856531831),
    (-15.7578458557458,-47.9242625792429),
    (-15.7787332586293,-47.9311234858603),
    (-15.7901882380251,-47.8948929040043),
    (-15.7855587432453,-47.8924876080930);

- **Comercial**
  - Comercial_1

    (-15.7953523872712,-47.8772355606754),
    (-15.7903405102228,-47.8729480612350),
    (-15.7872771965375,-47.8741093199739),
    (-15.7861752605043,-47.8806705634271),
    (-15.7853923715922,-47.8875178966789),
    (-15.7854616581640,-47.8919612955021),
    (-15.7902349057589,-47.8946575055660),
    (-15.7959647351997,-47.8953232001207),
    (-15.8013052128992,-47.8858829283661),
    (-15.8034192331949,-47.8787934670313),
    (-15.8018684244161,-47.8762789996385),
    (-15.7953523872712,-47.8772355606754);

- Comercial_2

(-15.7484179269408,-47.8799357573898),
(-15.7641859425557,-47.8750475141454),
(-15.7735898078348,-47.8730553255978),
(-15.7807847623818,-47.8728135411773),
(-15.7821259232371,-47.8679992217350),
(-15.7804255022872,-47.8655842700453),
(-15.7897236389623,-47.8605796745835),
(-15.7916642471866,-47.8571877814858),
(-15.7921572357420,-47.8562723974460),
(-15.7910791202718,-47.8275539788168),
(-15.7889599749195,-47.8270397659103),
(-15.7861898130227,-47.8298218238936),
(-15.7852916711109,-47.8374423494173),
(-15.7869753763154,-47.8444294057887),
(-15.7828641098327,-47.8545080053254),
(-15.7848056713168,-47.8578038936507),
(-15.7832112274056,-47.8590133038172),
(-15.7791819456402,-47.8587592433595),
(-15.7734718876049,-47.8619401898701),
(-15.7684814334476,-47.8607071908592),
(-15.7601612977949,-47.8602407311091),
(-15.7488853841207,-47.8706535169591),
(-15.7484179269408,-47.8799357573898);

- **Residencial**
  - Residencial_1

(-15.7860809823089,-47.8807349447240),
(-15.7870278124691,-47.8743360615762),
(-15.7830925634995,-47.8729701174298),
(-15.7733978595790,-47.8735642151932),
(-15.7676130179793,-47.8746286687134),
(-15.7610583168250,-47.8764551658899),
(-15.7478001158189,-47.8806134469192),
(-15.7395280122216,-47.8834293895555),
(-15.7342075237534,-47.8857870557475),
(-15.7312446599857,-47.8928503576503),
(-15.7316706172586,-47.8949622913294),
(-15.7380717763843,-47.8995031043119),
(-15.7514659983649,-47.8951845846253),
(-15.7626645442359,-47.8911626853498),
(-15.7725688638188,-47.8884877253869),
(-15.7785260358480,-47.8878245611176),
(-15.7852261291968,-47.8875141850514),
(-15.7860809823089,-47.8807349447240);

## ANEXO A – Especificações dos equipamentos utilizados

As especificações dos equipamentos são:

- **SL-D001 Dual Band 2,4GHz/5,8GHz 802.11a/b/g/n 300Mbps Wireless-N**
  - Modelo SL-D001
  - Interface USB
  - Padrões IEEE802.11 a / b / g / n
  - Chipset Ralink 3572
  - Taxa de dados 300Mbps
  - Canal de trabalho 1 ~ 13;
  - Segurança WPA / WEP / 802.1i
  - Potência 20dBm;
  - Frequência 2.4 ~ 2.4835GHz / 5 ~ 5.8GHz;
  - Antena Built-in 2T2R

- **COMFAST CFWU770N 802.11g/b/n 150Mbps USB Wi-Fi**
  - Marca COMFAST
  - Modelo CF-WU770N
  - Interface USB
  - Padrões IEEE802.11b/g/n
  - Chipset RT3070L
  - Taxas de dados 150Mbps
  - Segurança WPA-PSK / WPA2-PSK / WPA / WPA2, 64/128/152 bits de criptografia WEP
  - Frequência 2.4 ~ 2.4835GHz
  - Faixa de trabalho 1800m
  - Canal de trabalho 1 ~ 14;
  - Antena Direcional de 10dBi

- **USB 2.0 150Mbps 2.4GHz 802.11n Wi-Fi**
  - Padrões IEEE802.11b/g/n
  - Interface USB
  - Frequência 2,4 GHz
  - Taxa de dados 150Mbps
  - Chipset Ralink 3070
  - Antena externa
  - Canal de trabalho 1-14
  - Modo de trabalho Infra-estrutura e Ad-Hoc
  - Segurança WEP/WPA/WPA2/WPA-PSK/WPA2-PSK

- **SL-1506N Mini IEEE802.11b / g / n 150Mbps USB 2.0 Wi-Fi**
  - Modelo SL-1506N
  - Chipset Ralink 5370
  - Padrões IEEE 802.11 b / g / n Wi-Fi
  - Frequência 2,4 GHz
  - Taxa de dados 150Mbps
  - Segurança WEP/WPA/WPA2/WPA-PSK/WAP2-PSK

- **HOLUX M-1000C Receptor GPS Recarregável com Data Logger Bluetooth**
    - Criada em MTK MT3329 consumo de baixa potência chipset GPS
    - Memória Flash 4M bit para 200.000 gravação de dados de registro
    - 66 paralelas de localização por satélite canais para rápida aquisição e reaquisição
    - Sensibilidade Superior até -165 dBm.
    - Built-in WAAS, EGNPS Demodulador sem qualquer hardware adicional
    - Compatível com Bluetooth Serial Port Profile (SPP) completamente
    - Built-in bateria de ions de lítio mutável dura 20 horas
    - Bateria: recarregável Li-ion 850mAh, 3.7V